Cole - H02706 - 71 - P014917
(71)

AMERICAN
JOURNAL OF MATHEMATICS

FOUNDED BY THE JOHNS HOPKINS UNIVERSITY

EDITED BY

WEI-LIANG CHOW, THE JOHNS HOPKINS UNIVERSITY
HARISH-CHANDRA, COLUMBIA UNIVERSITY
ANDRÉ WEIL, UNIVERSITY OF CHICAGO
AUREL WINTNER, THE JOHNS HOPKINS UNIVERSITY

WITH THE COÖPERATION OF

L. V. AHLFORS
A. BOREL
H. CARTAN
S. S. CHERN
J. A. DIEUDONNÉ
P. HARTMAN
G. P. HOCHSCHILD
K. IWASAWA
F. I. MAUTNER
A. D. WALLACE

PUBLISHED UNDER THE JOINT AUSPICES OF
THE JOHNS HOPKINS UNIVERSITY
AND
THE AMERICAN MATHEMATICAL SOCIETY

510·5
007

VOLUME LXXIX

1957

CALCUTTA UNIVERSITY
CENTRAL LIBRARY

THE JOHNS HOPKINS PRESS
BALTIMORE 18, MARYLAND
U. S. A.

P14917

PRINTED IN THE UNITED STATES OF AMERICA
BY J. H. FURST COMPANY, BALTIMORE, MARYLAND

INDEX

PAGE

Abhyankar, Shreeram. On the finite factor groups of abelian groups of finite rational rank, ... 190

Abhyankar, Shreeram. Coverings of algebraic curves, . . . 825

Adler, Alfred. A characteristic relation in fibre bundles, . . 713

Aronszajn, N. On a problem of Weyl in the theory of singular Sturm-Liouville equations, ... 597

Aronszajn, N. and K. T. Smith. Characterization of positive reproducing kernels. Applications to Green's functions, . . 611

Baily, W. L. On the imbedding of V-manifolds in projective space, 403

Boas, R. P., Jr. and A. C. Schaeffer. Variational methods in entire functions, ... 857

Calderón, A. P. and A. Zygmund. Singular integral operators and differential equations, ... 901

Chern, Shiing-shen and Richard K. Lashof. On the total curvature of immersed manifolds, ... 306

Chern, Shiing-shen. A proof of the uniqueness of Minkowski's problem for convex surfaces, ... 949

Chow, Wei-Liang and Serge Lang. On the birational equivalence of curves under specialization, ... 649

Dieudonné, Jean. Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ (VI), ... 331

Dieudonné, Jean. On simple groups of type B_n, ... 922

Doss, Raouf. On mean motion, ... 389

Drazin, M. P. The nilpotence of nil subrings, ... 67

Dubins, L. E. On curves of minimal length with a constraint on average curvature, and with prescribed initial and terminal positions and tangents, ... 497

Gleason, Andrew and Richard S. Palais. On a class of transformation groups, ... 631

Grothendieck, A. Sur la classification des fibrés holomorphes sur la sphere de Riemann, ... 121

Hano, Jun-ichi. On Kaehlerian homogeneous spaces of unimodular Lie groups, ... 885

PAGE

Harish-Chandra. Differential operators on a semisimple Lie algebra, 87

Harish-Chandra. Fourier transforms on a semisimple Lie algebra I, 193

Harish-Chandra. Fourier transforms on a semisimple Lie algebra II, 653

Harish-Chandra. A formula for semisimple Lie groups, . . . 733

Hartman, Philip. On Jacobi brackets, ... 187

Hirschman, I. I., Jr. A note on entropy, ... 152

Hochschild, G. and G. D. Mostow. Extension of representations of Lie groups and Lie algebras, I, ... 924

Hoffman, Kenneth and I. M. Singer. Maximal subalgebras of $C(\Gamma)$, 295

Kan, Daniel M. On c.s.s. complexes, ... 449

Kelly, John B. Restricted bases, ... 258

Kervaire, Michel A. Relative characteristic classes, ... 517

Koecher, Max. Positivitätsbereiche im R^n, ... 575

Kuranishi, Masatake. On E. Cartan's prolongation theorem of exterior differential systems, ... 1

Kuranishi, Masatake. Errata, ... 448

Lang, Serge et Jean-Pierre Serre. Sur les revêtements non ramifiés des variétés algébriques, ... 319

Lang, Serge. See Wei-Liang Chow and Serge Lang, page 649.

Lang, Serge. Divisors and endomorphisms on an Abelian variety, . 761

Lashof, Richard K. See Chern and Lashof, page 306.

Matsusaka, T. The criteria for algebraic equivalence and the torsion group, ... 53

Milnor, John. Groups which act on S^n without fixed points, . . 623

Mostow, G. D. See G. Hochschild and G. D. Mostow, page 924.

Nassif, N. Note on convergence of the product of basic sets of polynomials, ... 943

Neugebauer, Christoph J. A characterization of the Lebesgue area, 73

Newns, W. F. Uniform spaces with unique structure, ... 48

O'Meara, O. T. Integral equivalence of quadratic forms in ramified local fields, ... 157

O'Meara, O. T. Local characterization of integral quadratic forms by Gauss sums, ... 687

Palais, Richard S. See Gleason and Palais, page 631.

PAGE

San Soucie, R. L. Weakly standard rings, ... 80

Schaeffer, A. C. See R. P. Boas, Jr. and A. C. Schaeffer, page 857.

Schechter, Martin. On estimating elliptic partial differential operators in the L_2 norm, ... 431

Serre, Jean-Pierre. See Lang et Serre, page 319.

Singer, I. M. See Hoffman and Singer, page 295.

Smith, K. T. See Aronszajn and Smith, page 611

Sternberg, Shlomo. On differential equations on the torus, . . 397

Sternberg, Shlomo. Local contractions and a theorem of Poincaré, 809

Sucheston, Louis. A note on conservative transformations and the recurrence theorem, ... 444

Wiener, Norbert and Aurel Wintner. On the non-vanishing of Euler products, ... 801

Wintner, Aurel. Bounded matrices and linear differential equations, 139

Wintner, Aurel. Ordinary differential equations and Laplace transforms, ... 265

Wintner, Aurel. On arithmetical summation processes, . . 559

Wintner, Aurel. On the existence of an absolute constant concerning "flat" oscillators, ... 710

Wintner, Aurel. Schwarz's lemma and a singularity of Briot-Bouquet, ... 778

Wintner, Aurel. Remarks to two previous papers (vol. 69, 1947, pp. 87-88 and vol. 71, 1949, pp. 587-594), ... 797

Wintner, Aurel. See Norbert Wiener and Aurel Wintner, page 801.

Wright, Fred B. Topological Abelian groups, ... 477

X. X. X. Correspondence, ... 951

Yang, Chung-Tao. On maps from spheres to Euclidean spaces, . 725

Zygmund, A. See A. P. Calderón and A. Zygmund, page 901.

ON E. CARTAN'S PROLONGATION THEOREM OF EXTERIOR DIFFERENTIAL SYSTEMS.*

By MASATAKE KURANISHI.

Introduction. The purpose of the present paper is to give necessary and sufficient conditions for E. Cartan's conjecture on the prolongations of exterior differential system ([1], p. 116) to be true. To begin with, we shall explain roughly what the problem is.

An exterior differential system is defined to be a finite set of homogeneous analytic differential forms on a domain D in a real euclidean space; analytic functions are considered as differential forms of degree 0. A submanifold D_1 of D is called an integral manifold (or integral, or solution), of the system if the differential forms on D_1 induced by those in the system are always zero forms. The main purpose of the theory of exterior differential systems is, it seems to the writer, to find an effective method to construct all integral manifolds and to clarify the structure of the set of all integral manifolds. The theory is essentially a theory of systems of partial differential equations. Namely, given a system of partial differential equations, for example $F_\alpha(x, y, z, \partial z/\partial x, \partial z/\partial y) = 0$, we construct, introducing new variables p and q, a differential system consisting of $F_\alpha(x, y, z, p, q)$, $dz - pdx - qdy$ on an appropriate domain in the five dimensional euclidean space (x, y, z, p, q). If D_1 is a two dimensional integral manifold of this system and if dx and dy are linearly independent on D_1, we can express the submanifold in the form $(x, y, z(x, y), p(x, y), q(x, y))$. Then the function $z(x, y)$ is a solution of the original equations. Conversely if $z(x, y)$ is a solution of the original equations, the submanifold $(x, y, z(x, y), [\partial z/\partial x](x, y), [\partial z/\partial y](x, y))$ is an integral manifold of the system.

The above observation suggests the following restriction to the problem. Fix a set of linearly independent Pfaffian forms $dx^1, \cdots, dx^p$ on D and restrict our attention to the integral manifolds on which $dx^1, \cdots, dx^p$ are linearly independent. In this case, the functions $x^1, \cdots, x^p$ will be called independent variables. In the present paper, we shall mainly concern ourselves with this restricted problem.

The problem, which is to find a general method to construct all integral manifolds, seems rather hard. Consequently, the results obtained so far are limited to furnish methods to construct integral manifolds satisfying some regularity conditions. For example, E. Cartan introduced the notion of general solutions of exterior differential systems and found a method to construct all general solutions. But unfortunately, there exist even examples of exterior differential systems which have integral manifolds but all the integral manifolds of the systems are not general solutions (cf. Example 1). Cartan's idea to proceed further starting from the theory of general solutions was to construct canonically new differential systems on new domains in such a way that the integral manifolds of the original systems correspond naturally in one-to-one manner to the integral manifolds of the newly constructed systems. If one constructs the new systems appropriately, it may possibly happen that an integral manifold of the original system which is not a general solution corresponds to a general solution of a newly constructed one.

---

* Received January 26, 1956.

For this purpose, E. Cartan defined the notion of prolongations of exterior differential systems, which is essentially to add partial derivatives of the unknown functions to the original systems of partial differential equations, and he said that, under certain conditions which are not easy to state precisely ([1], p. 116), every integral manifold will become a general solution after a finite number of prolongations. In the present paper, we shall justify this conjecture, giving a necessary and sufficient condition (cf. *Fundamental theorem,* § 6, Chapter III). Though E. Cartan considered two kinds of prolongations, that is, total and partial, we shall consider here only total prolongations. We shall also neglect the process of adding functions to the given system.

Since the theory developed so far is purely local, we shall restrict ourselves to differential systems on domains in real euclidean spaces. But it is easy to describe the theory on arbitrary real analytic manifolds, using the language in the theory of sheaves.

After some preliminaries, we shall summarize, in Chapter I, the Cartan-Kähler theory of exterior differential systems; except in a few cases the proofs are omitted. In Chapter II, we shall introduce the notion of normal exterior differential systems, and their prolongations will be examined. In Chapter III, after some preliminary notions are introduced and studied, the fundamental theorem will be formulated and proved.

Let me explain the expression "mod A," where A is a subspace of a vector space B. The writer uses this expression in two different meanings. By the first usage, it indicates the image in the factor space B/A by the natural mapping. For instance, $(b \bmod A)$, where b is an element of B, means the image of b in the factor space B/A by the natural mapping, and if he says "$b_1, \cdots, b_n$ are linearly independent $\bmod A$," he means that $(b_1 \bmod A), \cdots, (b_l \bmod A)$ are linearly independent. The second usage occurs when B is a subspace in a ring. For instance, "$b_1 \equiv b_2 \pmod{A}$" means that $b_1 - b_2$ is in the ideal generated by A. The meaning will always, we hope, be clear from the context.

The writer owes thanks to Professor S. Chern for a valuable suggestion on the theory of exterior differential systems, and to Professor T. Nakayama for useful suggestions on the algebraic tools in this paper. The writer was introduced to the theory of exterior differential systems in the seminar by Professor Y. Matsushima at Nagoya University, 1952-53 and the formulation of the theory in §§ 1-3 of Chapter I is mainly borrowed from his seminar. The writer wishes to express his grateful thanks to all of them.

1. Preliminaries. As for the fundamental concepts in the theory of manifolds we shall adopt the definitions given in C. Chevalley's book [4]. We shall consider exclusively real analytic manifolds, mainly domains in real euclidean spaces, which will be generally denoted by $\mathcal{V}$. We shall often omit the adjective "real." For a point x in $\mathcal{V}$, the tangent vector space at x to $\mathcal{V}$ will be generally denoted by $\mathcal{E}_x\mathcal{V}$. If $\mathcal{V}_1$ is a submanifold of $\mathcal{V}$ and x is in $\mathcal{V}_1$, $\mathcal{E}_x\mathcal{V}_1$ is a subspace of $\mathcal{E}_x\mathcal{V}$. Two submanifolds $\mathcal{V}_1$ and $\mathcal{V}_2$ of $\mathcal{V}$ passing through x are defined to be equivalent at x if there is an open neighborhood N of x in $\mathcal{V}$ such that $N \cap \mathcal{V}_1 = N \cap \mathcal{V}_2$. The equivalence class is called a germ of submanifolds of $\mathcal{V}$ at x. If a germ contains $\mathcal{V}_1$, $\mathcal{V}_1$ is called a representative of the germ. For any germ of submanifolds V at x, the tangent vector space to V, $\mathcal{E}V$, can be defined uniquely as the tangent vector space at x to a representative of V. A subset T in $\mathcal{V}$ is called a subvariety of $\mathcal{V}$, if for any point x of T there is an open neighborhood N of x and there is a set K of real analytic functions defined on N such that $T \cap N$ is equal to the common zeros of the functions in K. A subvariety is not necessarily the underlying space of a submanifold. A point x of a subvariety T is called a regular point of T if there is a neighborhood N of x in $\mathcal{V}$ such that $T \cap N$ is the underlying space of a submanifold. A subvariety T of $\mathcal{V}$ is called proper if $T \neq \mathcal{V}$. Remark that the empty set is a proper subvariety. By the classical theorem on the theory of analytic functions, it is clear that a proper subvariety of a (connected) manifold does not contain interior points of the manifold. Let f be an analytic mapping of a manifold $\mathcal{V}$ onto a manifold $\mathcal{V}_1$. Assume that for any point x of $\mathcal{V}_1$ there is an open neighborhood N of x and an analytic homeomorphism $g: N \times \mathcal{V}_2 \to f^{-1}(N)$, where $\mathcal{V}_2$ is a manifold independent of x, such that $(f \circ g)(x', v) = x'$ for any x' in N and v in $\mathcal{V}_2$, where $f \circ g$ is the composite mapping of f and g. In this case we shall say that f is a fiber mapping.

2. Let $\Lambda \mathcal{V}$ be the ring of real analytic differential forms on $\mathcal{V}$. Let $\Lambda^q \mathcal{V}$ be the module of homogeneous real analytic differential forms of degree q on $\mathcal{V}$. $\Lambda \mathcal{V}$ is the direct sum of $\Lambda^0 \mathcal{V}, \Lambda^1 \mathcal{V}, \cdots$, and $\Lambda^n \mathcal{V}$, where n is the dimension of $\mathcal{V}$. $\Lambda^0 \mathcal{V}$ is the ring of real analytic functions on $\mathcal{V}$. The exterior derivative and exterior product would be denoted by d and $\wedge$, respectively. Let θ be a differential form of homogeneous degree q defined on an open set N in $\mathcal{V}$. By defintion (p. 146 [4]), for each point x of N a q-multilinear function on $\mathcal{E}_x \mathcal{V}$ is assigned by θ. This function will be denoted by

$$\langle \theta, \mathcal{E}_x \mathcal{V} \rangle. \tag{1}$$

If $L_1, \cdots, L_q \in \mathcal{E}_x \mathcal{V}$, the value of $\langle \theta, \mathcal{E}_x \mathcal{V} \rangle$ at $L_1, \cdots, L_q$ will be denoted by $\langle \theta, L_1 \wedge \cdots \wedge L_q \rangle$. If $\theta = \theta_1 \wedge \cdots \wedge \theta_q$, then

$$\langle \theta, L_1 \wedge \cdots \wedge L_q \rangle = \det (\langle \theta_i, L_j \rangle).$$

For any subspace E of $\mathcal{E}_x \mathcal{V}$, the restriction of the function $\langle \theta, \mathcal{E}_x \mathcal{V} \rangle$ to E will be denoted by

$$\langle \theta, \mathcal{E} \rangle. \tag{2}$$

Let $\phi_1, \cdots, \phi_h$ be homogeneous differential forms defined on an open set containing x. Let E be a subspace of $\mathcal{E}_x \mathcal{V}$. If $\langle \phi_1, E \rangle, \cdots, \langle \phi_h, E \rangle$ are linearly independent multilinear functions, we shall say that $\phi_1, \cdots, \phi_h$ are linearly independent on E. If $\phi_1, \cdots, \phi_h$ are linearly independent on $\mathcal{E}_x \mathcal{V}$, we shall say that $\phi_1, \cdots, \phi_h$ are linearly independent at x.

Let f be an analytic mapping of $\mathcal{V}$ into $\mathcal{V}_1$. Let θ be a differential form on an open set N in $\mathcal{V}_1$. The differential forms on $f^{-1}(N)$ induced by f and θ will be denoted by $f^* \cdot \theta$, ($\delta f \cdot \theta$ by the notations in [4], cf. p. 151 [4]).

3. A q-dimensional subspace of $\mathcal{E}_x \mathcal{V}$ is called a q-dimensional contact element to $\mathcal{V}$ at x, and x its origin. The set of all q-dimensional contact elements to $\mathcal{V}$ at x, $'\mathcal{G}_x(\mathcal{V}, q)$, naturally forms an analytic manifold, the so-called Grassmannian manifold. There is a natural analytic manifold structure in $'\mathcal{G}(\mathcal{V}, q) = \bigcup \{'\mathcal{G}_x(\mathcal{V}, q); x \in \mathcal{V}\}$ such that $'\mathcal{G}_x(\mathcal{V}, q)$ is a submanifold of $'\mathcal{G}(\mathcal{V}, q)$ and such that the projection $\rho: {'\mathcal{G}}(\mathcal{V}, q) \to \mathcal{V}$ is an analytic fiber mapping, where ρ maps every contact element to its origin.

4. We shall construct the systems of coordinates of $'\mathfrak{S}(\mathfrak{V}, q)$ which will be used later frequently. Let $\omega^1, \cdots, \omega^q$ be analytic Pfaffian forms defined on a coordinate neighborhood N. Assume that $\omega^1, \cdots, \omega^q$ are linearly independent at each point in N. Set

$$(3) \qquad U(\omega^1, \cdots, \omega^q) = \{E \in {'\mathfrak{S}}(\mathfrak{V}, q)\,;\ \rho(E) \in N \text{ and } \omega^1, \cdots, \omega^q \text{ are linearly independent on } E\}.$$

Take analytic Pfaffian forms $\pi^1, \cdots, \pi^{n-q}$ such that $\omega^1, \cdots, \omega^q$, $\pi^1, \cdots, \pi^{n-q}$ form a base of Pfaffian forms on N. If $E \in U = U(\omega^1, \cdots, \omega^q)$, there is a unique system of real numbers $a_r^\sigma(E)$, $(r = 1, \cdots. q;\ \sigma = 1, \cdots n - q)$, such that

$$(4) \qquad \langle \pi^\sigma, E\rangle - \sum_{r=1}^{q} a_r^\sigma(E) \cdot \langle \omega^r, E\rangle = 0, \qquad (\sigma = 1, \cdots, n-q).$$

The functions a_r^σ are analytic functions on U and $(x^1 \circ \rho, \cdots, x^n \circ \rho, \cdots, a_r^\sigma, \cdots)$ a system of coordinates on U, where $(x^1, \cdots, x^n)$ is a system of coordinates on N. Moreover, this system gives a homeomorphism of U onto $N \times R^{q(n-q)}$, where $R^{q(n-q)}$ is a real euclidean space of $q(n-q)$ dimensions. If E' is in U, E' is equal to the set of all solutions of the following system of linear equations on $\mathcal{E}_{x'}\mathfrak{V}$:

$$(5) \qquad \langle \pi^\sigma, \mathcal{E}_{x'}\mathfrak{V}\rangle - \sum_{r=1}^{q} a_r^\sigma(E') \cdot \langle \omega^r, \mathcal{E}_{x'}\mathfrak{V}\rangle = 0, \qquad (\sigma = 1, \cdots, q),$$

where x' is the origin of E'. Let $L_1(E'), \cdots, L_q(E')$ be the tangent vectors in E', defined by the formulas:

$$(6) \qquad \langle \omega^s, L_r(E')\rangle = \delta_r^s, \qquad (r, s = 1, \cdots, q),$$

where δ_r^s is Kronecker's delta symbol. Then we have the equality:

$$(7) \qquad a_r^\sigma(E') = \langle \pi^\sigma, L_r(E')\rangle.$$

Let $\mathfrak{V}_1$ be a q-dimensional submanifold of $\mathfrak{V}$. The mapping T of $\mathfrak{V}_1$ into $'\mathfrak{S}(\mathfrak{V}, q)$, defined by the formula:

$$(8) \qquad T(x) = \mathcal{E}_x\mathfrak{V}_1, \qquad (x \in \mathfrak{V}_1),$$

is regular and locally univalent mapping. Thus T defines a submanifold of $'\mathfrak{S}(\mathfrak{V}, q)$, which will be denoted by $\mathcal{T}\mathfrak{V}_1$. If V_1 is a germ of q-dimensional submanifolds of $\mathfrak{V}$ at x, we can define the germ of submanifolds TV_1 in $'\mathfrak{S}(\mathfrak{V}, q)$ at $\mathcal{E}V_1$, taking a representative of V_1 and applying T. Define $'\mathfrak{S}^l(\mathfrak{V}, q)$ and $\mathcal{T}^l\mathfrak{V}_1$, $l = 1, 2, \cdots$, by the inductive formulas:

$$(8') \qquad \begin{aligned} &{'\mathfrak{S}^1}(\mathfrak{V}, q) = {'\mathfrak{S}}(\mathfrak{V}, q), \quad {'\mathfrak{S}^{l+1}}(\mathfrak{V}, q) = {'\mathfrak{S}}({'\mathfrak{S}^l}(\mathfrak{V}, q), q), \\ &\mathcal{T}^1\mathfrak{V}_1 = \mathcal{T}\mathfrak{V}_1, \qquad \mathcal{T}^{l+1}\mathfrak{V}_1 = \mathcal{T}(\mathcal{T}^l\mathfrak{V}_1). \end{aligned}$$

We can define $T^l V_1$ by similar formulas. $\mathcal{J}^l \mathcal{V}_1$ and $T^l V_1$ are submanifold and germ of submanifolds, respectively, of $'\mathcal{G}^l(\mathcal{V}, q)$.

Throughout this paper, let $\mathcal{V}$ be a (not necessarily bounded) connected domain in the real euclidean space.

Chapter I. Exterior Differential System.

1. **Exterior differential system.** *Definition* I. 1. An ideal Σ in the ring of real analytic differential forms on $\mathcal{V}$ is called an exterior differential system if it satisfies the following conditions:

(i) $d\Sigma \subset \Sigma$,

(ii) Σ is homogeneous, i. e., $\Sigma = \Sigma^{[0]} + \Sigma^{[1]} + \cdots + \Sigma^{[n]}$, where $\Sigma^{[i]} = \Sigma \cap \Lambda^i \mathcal{V}$ and n is the dimension of $\mathcal{V}$;

(iii) Σ is finitely generated, i. e., there is a finite number of forms $\theta_1, \cdots, \theta_\alpha$ in Σ such that Σ is generated, as an ideal, by $\theta_1, \cdots, \theta_\alpha$.

Let $\phi_1, \cdots, \phi_\beta$ be homogeneous differential forms on $\mathcal{V}$. The ideal in $\Lambda\mathcal{V}$ generated by $\phi_1, \cdots, \phi_\beta, d\phi_1, \cdots, d\phi_\beta$ is an exterior differential system, which is called the exterior differential system generated by $\phi_1, \cdots, \phi_\beta$.

Definition I. 2. A (q-dimensional) contact element E to $\mathcal{V}$ at x is called a (q-dimensional) integral element of Σ if and only if $\langle \theta, E \rangle = 0$ for every θ in Σ (cf. (2)). Let $'\mathcal{J}^q \Sigma$ be the set of all q-dimensional integral elements of Σ. A zero-dimensional integral element is sometimes called an integral point.

Take linearly independent Pfaffian forms $\omega^1, \cdots, \omega^q$ defined on an open set N. Set $U = U(\omega^1, \cdots, \omega^q)$, (cf. (3)). Then $E \in U$ is an integral element of Σ if and only if

$$\langle \theta, L_{r_1}(E) \wedge \cdots \wedge L_{r_a}(E) \rangle = 0 \tag{9}$$
$$(\theta \in \Sigma^{[a]}; r_1, \cdots, r_a = 1, \cdots, q; a = 0, 1, \cdots, q),$$

where, in the case $a = 0$, the left hand side of (9) means the value of the function θ at the origin of E. Hence, if we define the analytic function $K[\theta, q; r_1, \cdots, r_a]$ on U by the formula:

$$(K[\theta, q; r_1, \cdots, r_a])(E) = \langle \theta, L_{r_1}(E) \wedge \cdots \wedge L_{r_a}(E) \rangle, \tag{10}$$

and denote by $K(\Sigma; \omega^1, \cdots, \omega^q)$ the ideal in the ring $\Lambda^0 U$ of all real analytic functions on U generated by all such $K[\theta, q; r_1, \cdots, r_a]$, then $'\mathcal{J}^q E \cap U$ is equal to the set of common zeros of the functions in $K(\Sigma;\omega^1,\cdots,\omega^q)$. Therefore we have the following:

Proposition I.1. $'\mathfrak{I}^q\Sigma$ is a subvariety of $'\mathfrak{G}(\mathcal{V},\varsigma)$.

Definition I.3. Let T be a subvariety of $\mathcal{V}$ and x be a point of $\mathcal{V}$. Let K be a set of analytic functions defined on an open neighborhood N of x. The equation $K=0$ is called a local equation of T at x (or on N) if $N\cap T$ is equal to the set of common zeros of K.

Definition I.4. The equation: $K(\Sigma,\omega^1,\cdots,\omega^q)=0$ is called the canonical local equation of $'\mathfrak{I}^q\Sigma$ (on $U(\omega^1,\cdots,\omega^q)$).

Definition I.5. A submanifold $\mathcal{V}_1$ of $\mathcal{V}$ is called an integral manifold of Σ if, for each point x in $\mathcal{V}_1$ the tangent vector space to $\mathcal{V}_1$ at x is an integral element of Σ. A germ of submanifolds V_1 in $\mathcal{V}$ at x is called an integral at x if there is a representative of V_1 which is an integral manifold of Σ.

It is clear that $\mathcal{V}_1$ is an integral manifold of Σ if and only if the subring Σ_1 of $\Lambda\mathcal{V}_1$ which is the image of Σ under the dual mapping of the injection of $\mathcal{V}_1$ into $\mathcal{V}$ consists of only zero.

2. Polar equations, regular and ordinary integral elements. Let E be a q-dimensional contact element to $\mathcal{V}$ at x. Any vectors $L_1,\cdots,L_a$ in E and any form θ in $\Sigma^{[a+1]}$ define a linear functional $\theta[L_1,\cdots,L_a]$ on $\mathcal{E}_x\mathcal{V}$ by the formula:

$$(10')\qquad (\theta[L_1,\cdots,L_a])(L)=\langle\theta,L_1\wedge\cdots\wedge L_a\wedge L\rangle,\quad (L\in\mathcal{E}_x\mathcal{V}).$$

$\theta[L_1,\cdots,L_a]$ is equal to $\langle\theta,\mathcal{E}_x\mathcal{V}\rangle$, when $a=0$.

Definition I.6. The subspace of the conjugate space of $\mathcal{E}_x\mathcal{V}$ generated by all such $\theta[L_1,\cdots,L_a]$, $(\theta\in\Sigma^{[a+1]};\ L_1,\cdots,L_a\in E;\ a=0,1,\cdots,q$, will be called the system of polar forms of Σ at E and will be denoted by $J(\Sigma;E)$, (or by $J(E)$). The equation $J(E)=0$ is called the polar equation of Σ at E. The set of all solutions of this equation will be denoted by $H(E)$.

If E is an integral element of Σ, $H(E)$ contains E. It is easy to see the following:

Proposition I.2. Let E be an integral element of Σ. Let L be a tangent vector to $\mathcal{V}$ at the origin of E. Then the subspace spanned by E and L is an integral element of Σ if and only if L is in $H(E)$.

Proposition I.3. Let $\omega^1,\cdots,\omega^q$ be linearly independent Pfaffian forms on an open set N. Let $\theta_1, \cdots, \theta_\alpha$ be a system of generators (as an ideal) of Σ. If $E \in U(\omega^1, \cdots, \omega^q)$, the set

$$\{\theta_a[L_{i_1}(E), \cdots, L_{i_d}(E)]\,;\ a = 1, \cdots, \alpha;\ 0 \leqq i_1 \leqq \cdots \leqq i_d \leqq q;\ d = (\text{degree of } \theta_a) - 1 \geqq 0\}$$

is a system of generators of $J(E)$, (cf. (3) and (6)).

The dimension of the vector space $J(E)$ over the field R of real numbers will be denoted by $t(\Sigma; E)$, (or by $t(E)$), where t is considered as an integer valued function on ${}'\mathfrak{G}(\mathfrak{V}, q)$. If $E' \subseteq E$, the definition implies that $J(E') \subseteq J(E)$. Hence we have

Proposition I. 4. If $E' \subseteq E$, then $t(E') \leqq t(E)$. If $E \in {}'\mathfrak{I}^q\Sigma$, then $t(E) \leqq n - q$.

Definition I. 6. Let E be an element in ${}'\mathfrak{G}(\mathfrak{V}, q)$. Set

$$t_r(E) = \operatorname{Max}\{t(E')\,; E' \text{ is a } r\text{-dimensional subspace of } E\}. \qquad (r = 0, 1, \cdots, q).$$

Proposition I. 4 implies that $t_0(E) \leqq t_1(E) \leqq \cdots \leqq t_q(E) = t(E)$.

Definition I. 7. Let E be an element in ${}'\mathfrak{G}(\mathfrak{V}, q)$. Define integers $s_0(E), \cdots, s_q(E)$ by the formulas:

$$s_0(E) = t_0(E);\ s_r(E) = t_r(E) - t_{r-1}(E) \qquad (r = 1, \cdots, q-1),$$
$$s_q(E) = n - q - t_{q-1}(E).$$

$s_0(E), \cdots, s_q(E)$ is called the system of characters at E of Σ.

Denote by $\mathfrak{G}(E, r)$ the set of r-dimensional contact elements contained in E. $\mathfrak{G}(E, r)$ is a submanifold of ${}'\mathfrak{G}(E, r)$.

LEMMA I. 1. *The set of all* $E' \in \mathfrak{G}(E, r)$ *such that* $t(E') \leqq t_r(E)$ *is a proper subvariety of* $\mathfrak{G}(E, r)$.

Let T be a subvariety of an analytic manifold $\mathfrak{V}$. Let an equation: $K = 0$ be a local equation of T on an open set N (cf. Definition I. 3).

Definition I. 8. Let x be a point in $N \cap T$. K is called regular at x, if there are functions $f_1, \cdots, f_h$ in K such that the equation: $f_1 = \cdots = f_h = 0$ is a local equation of T on a neighborhood of x and such that $df_1, \cdots, df_h$ are linearly independent at x.

Now we shall define the notions of regular q-dimensional integral element of Σ by induction on q.

Definition I. 9. A point x of $'\mathfrak{I}^0\Sigma$ is called a regular zero-dimensional integral element if and only if there is a neighborhood N of x in $\mathcal{V}$ such that t is a constant function on $N \cap {'\mathfrak{I}^0\Sigma}$, $N \cap {'\mathfrak{I}^0\Sigma}$ is a submanifold of $\mathcal{V}$, and the equation $\Sigma^{[0]} = 0$ is a regular local equation of $'\mathfrak{I}^0\Sigma$ on N. A q-dimensional integral element $(q \geqq 1)$, is called regular if and only if

(i) E contains at least one regular $(q-1)$-dimensional integral element,

(ii) there is a neighborhood N of E in $'\mathfrak{G}(\mathcal{V}, q)$ such that t is a constant function on $N \cap {'\mathfrak{I}^q\Sigma}$.

Definition I. 10. An integral point x is called ordinary if and only if there is a neighborhood N of x in $\mathcal{V}$ such that $'\mathfrak{I}^0\Sigma \cap N$ is a submanifold and such that the equation: $\Sigma^{[0]} = 0$ on N is a regular local equation of $'\mathfrak{I}^0\Sigma \cap N$. A q-dimensional integral element E $(q \geqq 1)$, is called ordinary if and only if E contains at least one regular $(q-1)$-dimensional integral element.

Definition I. 11. Let E be a q-dimensional vector space. By a flag F on E we mean a chain of subspaces of E,

$$\{0\} = E_0 \subset E_1 \subset \cdots \subset E_r \subset \cdots \subset E_q = E,$$

where the dimension of E_r is r. E_r will be called the r-th component of the flag F. q is called the dimension of F. The set $\mathfrak{F}(E)$ of all flags on E forms a real analytic manifold. There is a natural manifold structure on $\mathfrak{F}(\mathcal{V}, q) = \bigcup \{F; F \in \mathfrak{F}(E), E \in {'\mathfrak{G}(\mathcal{V}, q)}\}$ such that $\mathfrak{F}(E)$ is a submanifold of $\mathfrak{F}(\mathcal{V}, q)$.

Let F be a flag on $E \in {'\mathfrak{G}(\mathcal{V}, q)}$. Let N_r be a neighborhood of the r-th component of F in $'\mathfrak{G}(\mathcal{V}, r)$.

$$(11) \qquad U(N_0, N_1, \cdots, N_q) = \{F' \in \mathfrak{F}(\mathcal{V}, q)\,;\ \text{the } r\text{-th component of } F' \text{ is in } N_r,\ r = 0, 1, \cdots, q\}.$$

Then all such $U(N_0, N_1, \cdots, N_q)$ form a fundamental system of neighborhoods of F in $\mathfrak{F}(\mathcal{V}, q)$.

Definition I. 12. Let E be an ordinary integral element. A flag F on E will be called regular if the r-th component of F is a regular integral element for $r = 0, 1, \cdots, q-1$.

We see easily the following

Proposition I. 5. Let E be an ordinary integral element of Σ. Then there exists at least one regular flag on E. The set of all regular flags of q dimensions forms an open set in $\mathfrak{F}(\mathfrak{V}, q) \cap \tau^{-1}('\mathfrak{J}^0\Sigma)$, where τ is the natural mapping of $\mathfrak{F}(\mathfrak{V}, q)$ onto $'\mathfrak{G}(\mathfrak{V}, q)$.

Set

$$(12) \quad \mathfrak{R}'\mathfrak{J}^q\Sigma = \{E \in {}'\mathfrak{G}(\mathfrak{V}, q)\,;\ E \text{ is a regular integral element of } \Sigma\}$$

$$(13) \quad \mathfrak{O}'\mathfrak{J}^q\Sigma = \{E \in {}'\mathfrak{G}(\mathfrak{V}, q)\,;\ E \text{ is an ordinary integral element of } \Sigma\}.$$

Clearly we have the relation: $\mathfrak{R}'\mathfrak{J}^q\Sigma \subseteq \mathfrak{O}'\mathfrak{J}^q\Sigma \subseteq {}'\mathfrak{J}^q\Sigma$.

THEOREM I. 1. *$\mathfrak{R}'\mathfrak{J}^q\Sigma$ and $\mathfrak{O}'\mathfrak{J}^q\Sigma$ are open subsets of $'\mathfrak{J}^q\Sigma$. Let E be an ordinary q-dimensional integral element of Σ. Then there is a neighborhood N of the origin of E such that $'\mathfrak{J}^0\Sigma \cap N$ is a submanifold. Let n_0 be the dimension of this submanifold. Let $\omega^1, \cdots, \omega^q$ be analytic Pfaffian forms on N which are linearly independent at each point in N, and which are also linearly independent on E. If N is sufficiently small, then there is a neighborhood $\mathfrak{N}$ of E in $'\mathfrak{G}(\mathfrak{V}, q)$ such that*

(i) *$'\mathfrak{J}^q\Sigma \cap \mathfrak{N}$ is a submanifold of dimension $\left(\sum_{r=1}^{q} r \cdot s_r(E)\right) + n_0$,*

(ii) *the equations $K(\Sigma, \omega^1, \cdots, \omega^q) = 0$ on $\mathfrak{N}$ is a regular local equation of $'\mathfrak{J}^q\Sigma \cap \mathfrak{N}$.*

(iii) *the restriction of the projection ρ on $'\mathfrak{J}^q\Sigma \cap \mathfrak{N}$ is a fiber mapping of $'\mathfrak{J}^q\Sigma \cap \mathfrak{N}$ onto $'\mathfrak{J}^0\Sigma \cap N$.*

The esential part of the theorem is due to Cartan [4]. The present formulation is due to Y. Matsushima (unpublished). This theorem will not be used in the remainder of the present paper.

Remark. $\mathfrak{O}'\mathfrak{J}^q\Sigma$ may be an empty set, even if $'\mathfrak{J}^q\Sigma$ is not empty, as in the following

Example 1. Let $\mathfrak{V}$ be the three-dimensional euclidean space with a system of coordinates (x, y, z). Denote by Σ the exterior system generated by $z \cdot dz$ and $z \cdot dx \wedge dy$. Then $'\mathfrak{J}^2\Sigma \neq \phi$, in fact, $z = 0$ is an integral manifold of Σ. The origin of any 2-dimensional integral element must satisfy the condition: $z = 0$, but such a point is not a regular integral point. Therefore it follows that $\mathfrak{O}'\mathfrak{J}^2\Sigma$ is empty.

The following proposition, which is a corollary of Theorem I. 1 will be used later. Therefore we shall prove it here directly.

Proposition I. 6. Let E be an ordinary q-dimensional integral element of Σ. Then, we can find a neighborhood N of the origin x of E in $\mathfrak{V}$ such that $N \cap {}'\mathfrak{J}^0\Sigma$ is a submanifold and such that there is an analytic mapping $f\colon N \cap {}'\mathfrak{J}^0\Sigma \rightarrow {}'\mathfrak{G}(\mathfrak{V}, q)$ satisfying the following conditions: (i) $f(x) = E$, (ii) $\rho \circ f =$ the identity mapping, and (iii) $f(N \cap {}'\mathfrak{J}^0\Sigma) \subseteq {}'\mathfrak{J}^q\Sigma$.

Proof. By definition, there is a neighborhood N_0 of x such that $N_0 \cap {}'\mathfrak{J}^0\Sigma$ is a submanifold. Let F be a regular flag on E. Let E_r $(r = 0, 1, \cdots, q)$, be the r-th component of F. It is sufficient to show the following statement $(\#)_r$ by induction on r $(r = 0, 1, \cdots, q)$:

$(\#)_r$: There is a neighborhood N_r of x such that $N_r \cap {}'\mathfrak{J}^0\Sigma$ is a submanifold and there is an analytic mapping f_r of $N_r \cap {}'\mathfrak{J}^0\Sigma$ into ${}'\mathfrak{G}(\mathfrak{V}, r)$ such that $f_r(x) = E_r$, $\rho \circ f_r =$ the identity mapping, and such that the image of f_r is in ${}'\mathfrak{J}^r\Sigma$.

$(\#)_0$ is trivial. Assume that $(\#)_{r-1}$ is proved. Let $\omega^1, \cdots, \omega^n$ be a base of Pfaffian forms on N_{r-1}. By Proposition I. 3, there are analytic functions A_{bj} $(b = 1, \cdots, h; j = 1, \cdots, n)$, on ${}'\mathfrak{G}(N_{r-1}, r-1)$ such that $\sum_{j=1}^{n} A_{bj}(E') \cdot \langle \omega^j, \mathcal{E}_x\mathfrak{V} \rangle$ $(b = 1, \cdots, h; x' = \rho(E'))$, generate $J(E')$ for any E' in ${}'\mathfrak{G}(N_{r-1}, r-1)$, (cf. Definition I. 6). By definition I. 9, there is a neighborhood N of E_{r-1} such that the dimension of $J(E')$ is constant when E' runs through N. Take a vector L in E_r but not in E_{r-1}. Then it follows that there is an analytic mapping $g\colon f_{r-1}(N_r \cap {}'\mathfrak{J}^0\Sigma) \rightarrow \mathcal{E}\mathfrak{V}$ (= the manifold of all tangent vectors to $\mathfrak{V}$) such that $\rho \circ g \circ f_{r-1} =$ the identity, $g(E_{r-1}) = L$, and such that $g(E') \in H(E')$ for any E' in $f_{r-1}(N_r \cap {}'\mathfrak{J}^0\Sigma)$, where N_r is a sufficiently small neighborhood of x contained in N_{r-1}. Adopting the system of coordinates mentioned in the preliminaries, we see easily that the mapping f_r of $N_r \cap {}'\mathfrak{J}^0\Sigma$ into ${}'\mathfrak{G}(\mathfrak{V}, r)$, defined by the formula: $f_r(x') = \{$the subspace spanned by $f_{r-1}(x')$ and $g \circ f_{r-1}(x')\}$, has the required properties.

3. E. Cartan's fundamental theorem.

THEOREM I. 2. *Let Σ be an exterior differential system on $\mathfrak{V}$. Let V_1 be an integral of Σ at x (Definition* I. 5). *Assume that $\mathcal{E}V_1 = E'$ is a regular integral element of Σ. Let E be a p-dimensional integral element of Σ, where $p-1$ is the dimension of V_1. Let V_2 be a germ of submanifolds in $\mathfrak{V}$. Suppose that they satisfy the following conditions:* (i) $E' \subset E$, (ii) *the dimension of $V_2 = n - s_{p-1}(E') + 1$, where n is the dimension of $\mathfrak{V}$,* (iii) $V_1 \subset V_2$, *and* (iv) $\mathcal{E}V_2 \cap H(E') = E$. *Then for any such E and V_2, there is a unique integral V_3 of Σ at x such that $\mathcal{E}V_3 = E$ and such that $V_1 \subset V_3 \subset V_2$.*

The theorem was first proved by E. Cartan, in the case Σ is generated as an ideal by $\Sigma^{[0]}$, $\Sigma^{[1]}$, and $\Sigma^{[2]}$. The general case was proved by E. Kähler [5]. The formulation of the theorem given here is due to E. Kähler.

Definition I. 13. An integral V_1 of Σ (at x) is called a general solution of Σ (at x) if $\mathcal{E}V_1$ is an ordinary integral element of Σ.

Remark 1. Theorem I. 2 (and its proof) provides an effective method to construct all general solutions at a regular integral point. The theorem is classically expressed by saying that, for any $(p-1)$-dimensional integral V_1 of Σ such that $\mathcal{E}V_1$ is a regular integral element and for any p-dimensional integral element E containing $\mathcal{E}V_1$, the set of all integrals whose tangent vector space is E, depends on $s_{p-1}(\mathcal{E}V_1)-1$ number of arbitrary functions of p variables. But it seems to the writer that some ambiguous points are left open about this notion.

4. Exterior differential system with independent variables.

Definition I. 14. A $\Lambda^0\mathfrak{V}$-submodule Ω of $\Lambda^1\mathfrak{V}$ is called a system of p independent variables if it satisfies the following conditions: there are analytic functions $f_1, \cdots, f_p$ on $\mathfrak{V}$ such that $\omega^1 = df_1, \cdots, \omega^p = df_p$ are linearly independent at each point in $\mathfrak{V}$ and such that Ω is $\Lambda^0\mathfrak{V}$-generated by $df_1, \cdots, df_p$. The set $\{\omega^1, \cdots, \omega^p\}$ is called a base of Ω.

Let n be the dimension of $\mathfrak{V}$. Then $\Lambda^1\mathfrak{V}$ itself is a system of n independent variables (since $\mathfrak{V}$ is a domain in a euclidean space).

Proposition I. 7. Let f be an analytic mapping of $\mathfrak{V}$ onto $\mathfrak{V}_1$. Let Ω be a system of p independent variables on $\mathfrak{V}_1$. Let $f^*\Omega$ be the $\Lambda^0\mathfrak{V}$-submodule generalted by all $f^*\omega$, where ω runs through the forms in Ω. Then $f^*\Omega$ is a system of p independent variables on $\mathfrak{V}$.

Set

$$\mathfrak{G}_\Omega(\mathfrak{V}, q) = \{E \in {}'\mathfrak{G}(\mathfrak{V}, q)\text{; the dimension of the vector space } \langle\Omega, E\rangle \text{ is equal to } q\}. \tag{14}$$

Then $\mathfrak{G}_\Omega(\mathfrak{V}, q)$ is an open submanifold of ${}'\mathfrak{G}(\mathfrak{V}, q)$. Let f be an analytic mapping of $\mathfrak{V}_1$ onto $\mathfrak{V}$. Then f induces an analytic mapping

$$d_q f\colon \mathfrak{G}_{f^*\Omega}(\mathfrak{V}_1, q) \rightarrow \mathfrak{G}_\Omega(\mathfrak{V}, q). \tag{15}$$

We shall write simply $\mathfrak{G}(\mathfrak{V}, q)$ instead of $\mathfrak{G}_\Omega(\mathfrak{V}, q)$, when there is no ambiguity about what a system of independent variables is considered.

Definition I. 15. A pair of exterior differential system Σ on $\mathcal{V}$ and a system of p independent variables Ω on $\mathcal{V}$ is called an exterior differential system with p independent variables and will be denoted by (Σ, Ω). p is called the number of independent variables in (Σ, Ω).

Definition I. 16. A q-dimensional integral element E of Σ is called an integral element of (Σ, Ω), if E is in $\mathcal{G}_\Omega(\mathcal{V}, q)$. By an integral manifold of (Σ, Ω), we mean a p-dimensional integral manifold $\mathcal{V}_1$ of (Σ, Ω) such that $\mathcal{E}_x\mathcal{V}_1$ is an integral element of (Σ, Ω) for each x in $\mathcal{V}_1$, where p is the number of independent variables in Ω. A germ of submanifolds is called an integral of (Σ, Ω) if it contains a representative which is an integral manifold of (Σ, Ω).

Set

$$\mathcal{J}^q(\Sigma, \Omega) = {}'\mathcal{J}^q\Sigma \cap \mathcal{G}_\Omega(\mathcal{V}, q), \tag{16}$$

$$\mathcal{O}\mathcal{J}^q(\Sigma, \Omega) = \mathcal{O}'\mathcal{J}^q\Sigma \cap \mathcal{G}_\Omega(\mathcal{V}, q), \tag{17}$$

$$\mathcal{R}\mathcal{J}^q(\Sigma, \Omega) = \mathcal{R}'\mathcal{J}^q\Sigma \cap \mathcal{G}_\Omega(\mathcal{V}, q). \tag{18}$$

Since $\mathcal{G}_\Omega(\mathcal{V}, q)$ is an open submanifold of ${}'\mathcal{G}(\mathcal{V}, q)$, Proposition I. 1 implies that $\mathcal{J}^q(\Sigma, \Omega)$ is a subvariety of $\mathcal{G}_\Omega(\mathcal{V}, q)$.

Let E be a contact element to $\mathcal{V}$ at x. $J(\Sigma; E)$ and $\langle \Omega, \mathcal{E}_x\mathcal{V} \rangle$ are subspaces of the vector space $\langle \Lambda^1\mathcal{V}, \mathcal{E}_x\mathcal{V} \rangle = (\mathcal{E}_x\mathcal{V})'$ (cf. Definition I. 6). Let f be the natural mapping of $(\mathcal{E}_x\mathcal{V})'$ onto $(\mathcal{E}_x\mathcal{V})'/\langle \Omega, \mathcal{E}_x\mathcal{V} \rangle$. Denote by $J(\Sigma, \Omega; E)$ the image of $J(\Sigma, E)$ by f. $J(\Sigma, \Omega; E)$ is called the system of reduced polar forms of E. The dimension of $J(\Sigma, \Omega; E)$ will be denoted by $t(\Sigma, \Omega; E)$ (or by $t(E, \Omega)$). If $E' \subseteq E$, then it follows that $t(E'; \Omega) \leqq t(E; \Omega)$.

Definition I. 6′. Let E be an element in $\mathcal{G}_\Omega(\mathcal{V}, q)$. Set $t_r(E) = \operatorname{Max}\{t(E', \Omega)\,;\ E' \text{ is a } r\text{-dimensional subspace of } E\}$, $(r = 0, 1, \cdots, q)$.

Then $t_0(E, \Omega) \leqq t_1(E, \Omega) \leqq \cdots \leqq t_q(E, \Omega) = t(E, \Omega)$.

Definition I. 7′. Let E be an element in $\mathcal{G}_\Omega(\mathcal{V}, q)$. Define integers $s_0(E, \Omega), \cdots, s_q(E, \Omega)$ by the formulas:

$$\begin{aligned} s_0(E, \Omega) &= t_0(E, \Omega), \\ s_r(E, \Omega) &= t_r(E, \Omega) - t_{r-1}(E, \Omega), \qquad (r = 1, \cdots, q-1), \\ s_q(E, \Omega) &= n - q - t_{q-1}(E, \Omega). \end{aligned}$$

$s_0(E, \Omega), \cdots, s_q(E, \Omega)$ is called the system of reduced characters at E of (Σ, Ω).

Definition I.17. Let (Σ, Ω) be an exterior differential system with p independent variables. Let x be an integral point of (Σ, Ω). (Σ, Ω) is called involutive at x if it satisfies the following conditions: (i) $\mathfrak{I}^p(\Sigma, \Omega) \cap \rho^{-1}(x)$ is not empty, (ii) $\mathfrak{I}^p(\Sigma, \Omega) \cap \rho^{-1}(x) \subseteq \mathfrak{O}\mathfrak{I}^p(\Sigma, \Omega)$.

5. Prolongations of exterior differential systems. Let Ω be a system of p independent variables on $\mathfrak{V}$. We shall write simply $\mathfrak{G}(\mathfrak{V}, p)$ instead of $\mathfrak{G}_\Omega(\mathfrak{V}, p)$. We remark that $\mathfrak{G}(\mathfrak{V}, p)$ is again a domain in the euclidean space of $n + p(n - p)$ dimensions (cf. 4. Preliminaries). Let ρ be the projection of $\mathfrak{G}(\mathfrak{V}, p)$ onto $\mathfrak{V}$. Denote by $\rho^* \cdot \Lambda^1\mathfrak{V}$ the $\Lambda^0\mathfrak{G}(\mathfrak{V}, p)$-submodule of $\Lambda^1\mathfrak{G}(\mathfrak{V}, p)$ generated by all $\rho^* \cdot \theta$, where θ runs through forms in $\Lambda^1\mathfrak{V}$. $\Lambda^0\mathfrak{G}(\mathfrak{V}, p)$ is, according to our general notations, the ring of real analytic functions on $\mathfrak{G}(\mathfrak{V}, p)$. Let E be an element in $\mathfrak{G}(\mathfrak{V}, p)$. Let L be a tangent vector to $\mathfrak{G}(\mathfrak{V}, p)$ at E (i.e., $L \in \mathcal{E}_E\mathfrak{G}(\mathfrak{V}, p)$). If $d\rho \cdot L = 0$ and if ψ is in $\rho^*\Lambda^1\mathfrak{V}$, then clearly $\langle \psi, L \rangle = 0$. Therefore a linear functional $\langle \psi. \mathcal{E}_x\mathfrak{V} \rangle_E$ on $\mathcal{E}_x\mathfrak{V}$, where x is the origin of E, is defined by the formula: $\langle \psi, \mathcal{E}_E\mathfrak{G}(\mathfrak{V}, p) \rangle = \langle \psi, \mathcal{E}_x\mathfrak{V} \rangle_E \circ d\rho$. The restriction of $\langle \psi, \mathcal{E}_x\mathfrak{V} \rangle_E$ to a subspace E' of $\mathcal{E}_x\mathfrak{V}$ will be denoted by $\langle \psi, E' \rangle_E$. If we write $\psi = \sum_{j=1}^{k} g_j \cdot \rho^*\theta^j$, where g_j are analytical functions on $\mathfrak{G}(\mathfrak{V}, p)$ and θ^j are analytic Pfaffian forms on $\mathfrak{V}$, then clearly $\langle \psi, E' \rangle_E = \sum_{j=1}^{k} g_j(E) \cdot \langle \theta^j, E' \rangle$. We shall write $\langle \psi, E \rangle$ instead of $\langle \psi, E \rangle_E$.

Definition I.18. Denote by $\Pi^{[1]}\Omega$ the set of all ψ in $\rho^*\Lambda^1\mathfrak{V}$ such that $\langle \psi, E \rangle = 0$ for all E in $\mathfrak{G}(\mathfrak{V}, p) = \mathfrak{G}_\Omega(\mathfrak{V}, p)$. Denote by $\Pi\Omega$ the ideal in $\Lambda\mathfrak{G}(\mathfrak{V}, p)$ generated by $\Pi^{[1]}\Omega$ and $d(\Pi^{[1]}\Omega)$. We shall see that $\Pi\Omega$ is an exterior differential system on $\mathfrak{G}(\mathfrak{V}, p)$. The exterior differential system with independent variables $(\Pi\Omega, \rho^*\Omega)$ will be called the associated differential system with Ω.

Let $\omega^1 = df_1, \cdots \omega^p = df_p$ be a base of Ω. Then it is obvious that $U(\omega^1, \cdots, \omega^p)$ (cf. (3)), is equal to $\mathfrak{G}(\mathfrak{V}, p)$. Therefore, if we choose analytic Pfaffian forms $\pi^1, \cdots, \pi^{n-p}$ such that $\omega^1, \cdots, \omega^p, \pi^1, \cdots, \pi^{n-p}$ form a base of $\Lambda^1\mathfrak{V}$, we may define a_i^σ, $(i = 1, \cdots, p;\ \sigma = 1, \cdots, n-p)$, on $\mathfrak{G}(\mathfrak{V}, p)$ by formula (4).

Proposition I.8. $\Pi^{[1]}\Omega$ is generated by $\rho^*\pi^\sigma - \sum_{i=1}^{p} a_i^\sigma \cdot \rho^*\omega^i$, $(\sigma = 1, \cdots, n-p)$.

Proof. Any ψ in $\rho^*\Lambda^1\mathfrak{V}$ can be written as $\psi = g_1 \cdot \rho^*\omega^1 + \cdots + g_p \cdot \rho^*\omega^p$

$+\, h_1 \cdot \rho^* \pi^1 + \cdots + h_{n-p} \cdot \rho^* \pi^{n-p}$, where g_i and h_σ are analtyic functions on $\mathcal{G}(\mathcal{V}, p)$. ψ is in $\Pi^{[1]}\Omega$ if and only if

$$0 = \sum_{i=1}^{p} g_i(E) \cdot \langle \omega^i, E \rangle + \sum_{\sigma=1}^{n-p} h_\sigma(E) \cdot \langle \pi^\sigma, E \rangle$$

$$= \sum_{i=1}^{p} \Big(g_i(E) + \sum_{\sigma=1}^{n-p} h_\sigma(E) \cdot a_i^\sigma(E) \Big) \langle \omega^i, E \rangle$$

for any E in $\mathcal{G}(\mathcal{V}, p)$. Therefore $g_i = -\sum_{\sigma=1}^{n-p} h_\sigma \cdot a_i^\sigma$. Thus ψ is in $\Pi^{[1]}\Omega$ if and only if $\psi = \sum_{\sigma=1}^{n-p} h_\sigma \cdot (\rho^* \pi^\sigma - \sum_{i=1}^{p} a_i^\sigma \cdot \rho^* \omega^i)$.

Proposition I. 8 implies, in particular, that $\Pi\Omega$ is an exterior differential system.

THEOREM I. 3. *Let Ω be a system of p independent variables. If $\mathcal{V}_1$ is a p-dimensional submanifold of $\mathcal{V}$ such that $\mathcal{E}_x \mathcal{V}_1 \in \mathcal{G}(\mathcal{V}, p)$ for any x in $\mathcal{V}_1$, then $\mathcal{J}\mathcal{V}_1$ (cf. (8)) is an integral manifold of $(\Pi\Omega, \rho^*\Omega)$. Conversely, if V_1^* is an integral of $(\Omega\Pi, \rho^*\Omega)$, then there is a unique germ of submanifolds $\mathcal{V}_1$ of $\mathcal{V}$ such that $\mathcal{J}\mathcal{V}_1 = \mathcal{V}^*$.*

Proof. The first half of the theorem is almost obvious by the formula (4) and Proposition I. 8. As for the second half, let $\mathcal{V}_1^*$ be an integral manifold of $(\Pi\Omega, \rho^*\Omega)$. Then if E is in $\mathcal{V}_1^*$, then $\langle \pi^\sigma, d\rho \cdot (\mathcal{E}_E \mathcal{V}_1^*) \rangle - \sum_{i=1}^{p} a_i^\sigma(E) \cdot \langle \omega^i, d\rho \cdot (\mathcal{E}_E \mathcal{V}_1^*) \rangle = 0$. By (5), it follows that $d\rho \cdot (\mathcal{E}_E \mathcal{V}_1^*) \subseteq E$. Since $\mathcal{E}_E \mathcal{V}_1^*$ is in $\mathcal{G}_{\rho^*\Omega}(\mathcal{G}(\mathcal{V}, p), p)$, it follows that $d\rho \cdot (\mathcal{E}_E \mathcal{V}_1^*)$ is p-dimensional. Hence $d\rho \cdot (\mathcal{E}_E \mathcal{V}_1^*) = E$. And locally $d\rho$ is univalent. Therefore $\rho : \mathcal{V}_1^* \rightarrow \mathcal{V}$ defines a submanifold $\mathcal{V}_1$ of $\mathcal{V}$. For any E in $\mathcal{V}_1^*$, $\mathcal{E}_{\rho(E)} \mathcal{V}_1 = d\rho \cdot (\mathcal{E}_E \mathcal{V}_1^*) = E$. Thus $\mathcal{V}_1^* = \mathcal{J}\mathcal{V}_1$. In the above proof, $\mathcal{V}_1$ is not a submanifold in the strict sense, because $d\rho$ is only locally univalent. But what matters here is the germs determined by $\mathcal{V}_1^*$. Therefore this point does not matter in this proof.

Let $\omega^1, \cdots, \omega^p$ be a base of Ω. Then the ideal $K(\Sigma; \omega^1, \cdots, \omega^p)$, (cf. (10)), in the ring of analytic functions on $U(\omega^1, \cdots, \omega^p) = \mathcal{G}(\mathcal{V}, p)$ does not depend on the choice of the base. Let us denote this ideal by $K(\Sigma, \Omega)$. We showed that $K(\Sigma, \Omega)$ is finitely generated. Let $\mathcal{P}_\Omega \Sigma$ be the exterior differential system on $\mathcal{G}_\Omega(\mathcal{V}, p) = \mathcal{G}(\mathcal{V}, p)$ generated by $K(\Sigma, \Omega)$ and $\Pi\Omega$.

Definition I. 19. *Let* (Σ, Ω) be an exterior differential system with independent variables on $\mathcal{V}$. The exterior differential system with independent variables $(\mathcal{P}_\Omega \Sigma, \rho^*\Omega)$ on $\mathcal{G}_\Omega(\mathcal{V}, p)$ is called the prolongation of (Σ, Ω), and will be denoted by $\mathfrak{P}(\Sigma,\Omega)$. The l-th iteration of prolongations will be denoted by $\mathfrak{P}^{l}(\Sigma,\Omega)$.

Proposition I. 9. $'\mathfrak{S}^0\mathfrak{P}_\Omega\Sigma=\mathfrak{S}^p(\Sigma,\Omega)$, where p is the number of independent variables in (Σ,Ω).

The proof is obvious by the definitions.

THEOREM I. 4. *Let* (Σ,Ω) *be an exterior differential system with independent variables. If* $\mathfrak{V}_1$ *is an integral manifold of* (Σ,Ω), $\mathfrak{J}\mathfrak{V}_1$ *is an integral manifold of* $\mathfrak{P}(\Sigma,\Omega)$. *Conversely, if* $\mathfrak{V}_1{}^*$ *is an integral of* $\mathfrak{P}(\Sigma,\Omega)$, *there is a unique germ of submanifolds* $\mathfrak{V}_1$ *of* $\mathfrak{V}$ *such that* $\mathfrak{J}\mathfrak{V}_1=\mathfrak{V}^*$. *Then* $\mathfrak{V}_1$ *is automatically an integral manifold of* (Σ,Ω).

Proof. Let $\mathfrak{V}_1$ be an integral manifold of (Σ,Ω). Then $\mathfrak{J}\mathfrak{V}_1\subseteq{}'\mathfrak{S}^0\mathfrak{P}_\Omega\Sigma=\mathfrak{S}^p(\Sigma,\Omega)$, where p is the number of independent variables. By Theorem I. 3, $\mathfrak{J}\mathfrak{V}_1$ is an integral manifold of $(\Pi\Omega,\rho^*\Omega)$. Then it follows that $\mathfrak{J}\mathfrak{V}_1$ is an integral manifold of $\mathfrak{P}(\Sigma,\Omega)$. Let $\mathfrak{V}_1{}^*$ be an integral manifold of $\mathfrak{P}(\Sigma,\Omega)$. Then $\mathfrak{V}_1{}^*$ is an integral manifold of $(\Pi\Omega,\rho^*\Omega)$. Therefore, by Theorem I. 3, there is a unique submanifold $\mathfrak{V}_1$ of $\mathfrak{V}$ such that $\mathfrak{J}\mathfrak{V}_1=\mathfrak{V}_1{}^*$. Since $\mathfrak{J}\mathfrak{V}_1=\mathfrak{V}_1{}^*\subseteq{}'\mathfrak{S}^0\mathfrak{P}_\Omega\Sigma=\mathfrak{S}^p(\Sigma.\Omega)$, $\mathfrak{V}_1$ is an integral manifold of (Σ,Ω). Here we assumed that $\mathfrak{V}_1{}^*$ is a sufficiently small representative of $V_1{}^*$.

THEOREM I. 5. *Let* (Σ,Ω) *be an exterior differential system with* p *independent variables on* $\mathfrak{V}$. *Let* E^* *be a* p*-dimensional integral element of* $\mathfrak{P}(\Sigma,\Omega)$. *If, moreover,* $d\rho\cdot E^*$ *is an ordinary integral element, we have the following relations:*

$$s_q(E^*)=\sum_{r=q}^{p}s_r(E),\qquad (E=d\rho\cdot E^*;\ q=1,\cdots,p).$$

This theorem was proved by E. Cartan [2] in the case where Σ is generated by $\Sigma^{[0]}$, $\Sigma^{[1]}$, and $d\Sigma^{[1]}$. The general case was proved by Y. Matsushima [6].

Remark. The theorem shows that, if E is an ordinary integral element of (Σ,Ω), any integral element E^* of $\mathfrak{P}(\Sigma,\Omega)$ such that $d\rho\cdot E^*=E$ is ordinary. But the ordinarity of E^* does not imply that of E.

The following lemma, which is easy to prove, is often useful in calculating prolongations.

LEMMA I. 2. *Let* (Σ,Ω) *be exterior differential system. Let* $\omega^1,\cdots,\omega^p$ *be a base of* Ω. *Then the functions* $K[\theta,p;r_1,\cdots,r_a]=K_{r_1\cdots r_a}$ *on*

$\mathcal{G}_\Omega(\mathcal{V}, p) = U(\omega^1, \cdots, \omega^p)$, *defined by formula* (10), *where* a *is the degree of the differential form* θ, *are uniquely determined by the following formula*:

$$(19) \qquad \rho^*\theta \equiv \sum_{1 \leqq r_1 < \cdots < r_a \leqq p} K_{r_1 \cdots r_a} \cdot \rho^*\omega^{r_1} \wedge \cdots \wedge \rho^*\omega^{r_a} \qquad (\operatorname{mod} \Pi^{[1]}\Omega).$$

Chapter II. Normal Exterior Differential System.

1. Normal exterior differential system.

Definition II. 1. An exterior differential system with independent variables (Σ, Ω) on a real analytic manifold $\mathcal{V}$ is called normal if it satisfies the following conditions

(i) $\Sigma^{[0]} = 0$;

(ii) there are analytic Pfaffian forms $\theta^1, \cdots, \theta^{\alpha_1}$ on $\mathcal{V}$ which form a system of generators of $\Sigma^{[1]}$ and which are linearly independent modulo Ω at each point in $\mathcal{V}$;

(iii) $\Sigma^{[2]} \equiv 0$; $(\operatorname{mod} \Omega + \Sigma^{[1]})$

(iv) Σ is generated as an ideal by $\Sigma^{[1]}$ and $\Sigma^{[2]}$.

THEOREM II. 1. *Let* (Σ, Ω) *be an exterior system with* p *independent variables on* $\mathcal{V}$. *Then* $\mathcal{P}(\Sigma, \Omega)$ *satisfies the conditions* (iii) *and* (iv) *in Definition* II. 1.

Therefore, if $\mathcal{S}^p(\Sigma, \Omega)$ forms a submanifold on a neighborhood N of a p-dimensional element, restricting $\mathcal{P}(\Sigma, \Omega)$ on N, we may obtain in general a normal exterior system with independent variables. For this reason, we shall restrict our attention to a normal exterior differential system with independent variables. Of course, there are many systems which cannot be treated by the theory of normal systems. We shall say simply normal system instead of normal exterior differential system with independent variables.

Our next concern is to express $\mathcal{P}^l(\Sigma, \Omega)$ more explicitly. To do this we shall restrict $\mathcal{P}^l(\Sigma, \Omega)$ on a submanifold of $\mathcal{G}^l(\mathcal{V}, p)$ which contains $\mathcal{S}^0\mathcal{P}^l(\Sigma, \Omega)$, and we shall write down explicitly the systems and their systems of polar forms.

2. Admissible restriction. Let Σ be an exterior differential system on $\mathcal{V}$. Let $f_1, \cdots, f_c$ be analytic functions in $\Sigma^{[0]}$ such that $df_1, \cdots, df_c$ are linearly independent at each point in $\mathcal{V}$. Let $\mathcal{V}'$ be the submanifold of

$\mathfrak{V}$ defined by the conditions: $f_1 = \cdots = f_c = 0$. Σ induces an exterior differential system Σ' on $\mathfrak{V}'$. Σ' is called an admissible restriction of Σ and c is called the character of the admissible restriction. Let Ω be a system of p independent variables on $\mathfrak{V}$. Denote by Ω' the $\Lambda^0\mathfrak{V}'$-submodule generated by the restriction of Ω to $\mathfrak{V}'$. If Ω' is a system of p independent variables, we shall say that (Σ', Ω') is an admissible restriction of (Σ, Ω), and that c is the character of the restriction.

Proposition II. 1. Let (Σ', Ω') on $\mathfrak{V}'$ be an admissible restriction of (Σ, Ω) on $\mathfrak{V}$. For $q = 0, 1, \cdots, \dim \mathfrak{V}$, denote by i_q the injection of $\mathfrak{G}_{\Omega'}(\mathfrak{V}', q)$ into $\mathfrak{G}_{\Omega}(\mathfrak{V}, q)$ induced by the injection i of $\mathfrak{V}'$ into $\mathfrak{V}$. Then i_q induces a homeomorphism of $\mathfrak{J}^q(\Sigma', \Omega')$ onto $\mathfrak{J}^q(\Sigma, \Omega)$. If E is an element of $\mathfrak{J}^q(\Sigma', \Omega')$, then $s_0(i_q(E)) + c = s_0(E)$ and $s_r(i_q(E)) = s_r(E)$ for $r = 1, \cdots, q$, where c is the character of the restriction.

Proof. Let (Σ', Ω') be an admissible restriction by the functions $f_1, \cdots, f_c$ in $\Sigma^{[0]}$. The first half of the proposition follows from the fact that f_j and df_j, $(j = 1, \cdots, c)$, are in Σ. Let x be an integral point of Σ'. Let i^* be the linear mapping of $\langle \Lambda^1\mathfrak{V}, \mathcal{E}_x\mathfrak{V} \rangle$ onto $\langle \Lambda^1\mathfrak{V}', \mathcal{E}_x\mathfrak{V}' \rangle$ induced by i. Then the kernel of i^* is the subspace generated by $\langle df_1, \mathcal{E}_x\mathfrak{V} \rangle, \cdots \langle df_c, \mathcal{E}_x\mathfrak{V} \rangle$. Hence $t(\Sigma', x) + c = t(\Sigma, i(x))$. Assume that $t(\Sigma', E_1) + c = t(\Sigma, i(E_1))$ for any E_1 in $\mathfrak{G}_{\Omega}(\mathfrak{V}', r)$ for $r = 1, \cdots, q-1$. Let E be an element in $\mathfrak{G}_{\Omega}(\mathfrak{V}, q)$. Take a $(q-1)$-dimensional subspace E_1 of E. Then i^* induces a mapping $J(i(E))/J(i(E_1))$ onto $J(E)/J(E_1)$. The kernel of i^* is in $J(\Sigma, i(x)) \subseteq J(\Sigma, i(E_1))$, where x is the origin of E. Hence

$$J(\Sigma, i(E))/J(\Sigma, i(E_1)) \approx J(\Sigma', E)/J(\Sigma', E_1).$$

Therefore, using the assumption of induction, we see that $t(\Sigma', E) + c = t(\Sigma, i(E))$. Then, by Definition I. 7, we can easily deduce the second half of the proposition.

Proposition II. 2. Let (Σ', Ω') on $\mathfrak{V}'$ be an admissible restriction of (Σ, Ω) on $\mathfrak{V}$. Let c be the character of the restriction. We can naturally identify $\mathfrak{G}_{\Omega'}(\mathfrak{V}', p)$ to a submanifold of $\mathfrak{G}_{\Omega}(\mathfrak{V}, p)$, where p is the number of independent variables. Then $\mathfrak{P}(\Sigma', \Omega')$ is an admissible restriction of $\mathfrak{P}(\Sigma, \Omega)$ and its character is equal to $c(p+1)$.

Proof. Let $\omega^1, \cdots, \omega^p$ be a base of Ω. Then $\mathfrak{G}_{\Omega}(\mathfrak{V}, p) = U(\omega^1, \cdots, \omega^p)$. To construct a system of coordinates on $U(\omega^1, \cdots, \omega^p)$, we can choose $\pi^1, \cdots, \pi^{n-p}$ such that $\pi^1 = df_1, \cdots, \pi^c = df_c$ (cf. **4.** in Preliminaries). Then $\mathfrak{G}_{\Omega'}(\mathfrak{V}', p)$ is the submanifold defined by the system of equations (*):

$f_1=\cdots=f_c=a_r{}^j=0$ $(r=1,\cdots,p\,;j=1,\cdots,c)$. Since df_j is in $\Sigma^{[1]}$, the functions $a_r{}^j$ are in $\mathcal{P}(\Sigma,\Omega)$. Hence (*) defines an admissible restriction $\mathcal{P}(\Sigma,\Omega)'$ of $\mathcal{P}(\Sigma,\Omega)$ and its character is $c(p+1)$. It remains to prove that $\mathcal{P}(\Sigma,\Omega)'=\mathcal{P}(\Sigma',\Omega')$. This can be done by writing down the elements in $\mathcal{P}(\Sigma',\Omega')$ and $\mathcal{P}(\Sigma,\Omega)'$.

Proposition II. 3. Let (Σ',Ω') be an admissible restriction of (Σ,Ω). Let (Σ'',Ω'') be an admissible restriction of (Σ',Ω'). Let c' and c'' be their characters. Then (Σ'',Ω'') is an admissible restriction of (Σ,Ω) and its character is $c'+c''$.

The proof is easy.

3. The exterior differential system $\mathcal{R}_l\Sigma$. Let (Σ,Ω) be a normal system on $\mathfrak{V}$. Let $\omega^1,\cdots,\omega^p$ be a base of Ω. Remark that $d\omega^i=0$ by Definition I. 14. We can choose a base $\omega^1,\cdots,\omega^p$, $\theta^1,\cdots,\theta^{\alpha_1}$, $\varpi^1,\cdots,\varpi^m$ of Pfaffian forms on $\mathfrak{V}$ such that $\theta^1,\cdots,\theta^{\alpha_1}$ generate $\Sigma^{[1]}$, and $d\varpi^\lambda=0$. Throughout § 2 and § 3, we shall fix a base. Let $u^\lambda{}_{i_1\cdots i_l}$, $(\lambda=1,\cdots,m\,;$ $i_1,\cdots,i_l=1,\cdots,p\,;$ $l=1,2,\cdots)$, be a system of indeterminates under the conditions: $u^\lambda{}_{i_1\cdots i_l}=u^\lambda{}_{j_1\cdots j_l}$, where $j_1,\cdots,j_l$ is any permutation of $i_1,\cdots,i_l$. We can consider $u^\lambda{}_{i_1\cdots i_l}$, for a fixed l, as a system of coordinates in euclidean space R_l of dimension $n_l=m\cdot C_l{}^{p+l-1}$, where $C_b{}^a$ is the binomial coefficient. Set $R_0=\mathfrak{V}$ and $n_0=$ the dimension of $\mathfrak{V}$.

Set $\mathcal{R}_l=R_0\times R_1\times\cdots\times R_l$ $(l\geqq 0)$. We have the projection $\rho_{l'}{}^l$: $\mathcal{R}_l\rightarrow\mathcal{R}_{l'}$ for $l\geqq l'$. To avoid inessential complications of notations, let us omit the symbols $\circ\rho_{l'}{}^l$, $(\rho_{l'}{}^l)^*$, as far as confusion may not occur. For example, if f is a function on $\mathcal{R}_{l'}$, f automatically means also the functions $f\circ\rho_{l'}{}^l$ on $\mathcal{R}_l$ for any $l\geqq l'$. The same rule will be applied to differential forms. When we want to indicate on what manifold f is considered, we shall say f on $\mathcal{R}_l$, for example.

Let Π_l be the $\Lambda^0\mathcal{R}_l$-submodule of $\Lambda^1\mathcal{R}_l$ generated by the following set (Π_l) of Pfaffian forms on $\mathcal{R}_l$:

$$\theta^\alpha,\quad(\alpha=1,\cdots,\alpha_1),$$

$$(\Pi_l)\qquad {}^*\varpi^\lambda=\varpi^\lambda-\sum_{i=1}^{p}u^\lambda{}_i\cdot\omega^i,\ {}^*\varpi^\lambda{}_{k_1}=du^\lambda{}_{k_1}-\sum_{i=1}^{p}u^\lambda{}_{k_1i}\cdot\omega^i,\cdots,$$

$${}^*\varpi^\lambda{}_{k_1\cdots k_\nu}=du^\lambda{}_{k_1\cdots k_\nu}-\sum_{i=1}^{p}u^\lambda{}_{k_1\cdots k_\nu i}\cdot\omega^i,\ \cdots,$$

$$\varpi^\lambda{}_{k_1\cdots k_{l-1}}=du^\lambda{}_{k_1\cdots k_{l-1}}-\sum_{i=1}^{p}u^\lambda{}_{k_1\cdots k_{l-1}i}\cdot\omega^i,$$

$$(\lambda=1,\cdots,m\,;k_1,\cdots,k_{l-1}=1,\cdots,p\,;\nu=1,\cdots,l-1).$$

We shall consider ${}^*\varpi^\lambda$ as the case $\nu=0$ of ${}^*\varpi^\lambda{}_{k_1\cdots k_\nu}$. It is obvious that $\omega^1,\cdots,\omega^p$, the elements of $(\Pi_l)'$, and $du_{k_1\cdots k_l}$ form a base of Pfaffian forms on $\mathcal{R}_l$. Thus

$$\dim\langle\Pi_l,\mathcal{E}_y\mathcal{R}_l\rangle+p=\sum_{\nu=0}^{l-1}n_\nu=\dim\mathcal{R}_{l-1} \tag{20}$$

for any y in $\mathcal{R}_l$. If f is a function on $\mathcal{R}_{l-1}$, $d(f\circ\rho_{l-1}{}^l)$ is in $(\rho_{l-1}{}^l)^*\Lambda^1\mathcal{R}_{l-1}$. Therefore, for any function f on $\mathcal{R}_{l-1}$, we can define the function $D_k{}^l\cdot f$, $(k=1,\cdots,p)$, on $\mathcal{R}_l$ by the formula:

$$d(f\circ\rho_{l-1}{}^l)\equiv\sum_{k=1}^{p}(D_k{}^l\cdot f)\cdot\omega^k\ (\operatorname{mod}\Pi_l). \tag{21}$$

It is easy to see that, if $l_1\geqq l$, $D_k{}^{l_1}(f\circ\rho_{l-1}{}^{l_1-1})=(D_k{}^l\cdot f)\circ\rho_l{}^{l_1}$. Hence we may omit the index l and simply write $D_k\cdot f$. Let D_k be the mapping of the vector space of analytic functions on $\mathcal{R}_{l-1}$ to that on $\mathcal{R}_l$ of which value at f is $D_k\cdot f$. Since $d(d(f\circ\rho_{l-1}{}^l)=0$,

$$D_k\circ D_h=D_h\circ D_k,\qquad (h,k=1,\cdots,p). \tag{22}$$

Clearly, they have the usual properties of differentiation. For example,

$$D_k\cdot(f\cdot g)=(D_k\cdot f)\cdot g+f\cdot(D_k\cdot g). \tag{23}$$

By the condition (ii) of the normal system, we can write, for any ϕ in $\Sigma^{[2]}$,

$$\phi\equiv\sum_{i=1}^{p}\sum_{\lambda=1}^{m}A_{\phi\,;i\lambda}\omega^i\wedge\varpi^\lambda+\sum_{i=1}^{p}\sum_{j=1}^{p}\tfrac{1}{2}B_{\phi\,;ij}\omega^i\wedge\omega^j\quad(\operatorname{mod}\Sigma^1) \tag{24}$$

where $A_{\phi\,;\alpha}$ and $B_{\phi\,;ij}$ are analytic functions on $\mathcal{V}$ and $B_{\phi\,;ij}+B_{\phi\,;ji}=0$. Set

$$\Theta_{\phi\,;ij\,;}=\sum_{\lambda=1}^{m}(A_{\phi\,;i\lambda}\cdot u_j{}^\lambda-A_{\phi\,;j\lambda}\cdot u_i{}^\lambda)+B_{\phi\,;ij}. \tag{25}$$

They are analytic functions on $\mathcal{R}_l$ for $l\geqq 1$. Starting from $\Theta_{\phi\,;ij\,;}$, we shall define analytic functions $\Theta_{\phi\,;ij\,;k_1\cdots k_{l-1}}$ $(i,j,k_1,\cdots,k_{l-1}=1,\cdots,p)$ on $\mathcal{R}_{l'}$ $(l'\geqq l)$, by the formula:

$$\Theta_{\phi\,;ij\,;k_1\cdots k_{l-1}}=D_{k_{l-1}}\circ\cdots\circ D_{k_2}\circ D_{k_1}(\Theta_{\phi\,;ij\,;}). \tag{26}$$

For simplicity, we shall denote by $\mathcal{K}_l$ the set $k_1,\cdots,k_l$. $\mathcal{K}_lk$, $k\mathcal{K}_l$ means the set $k_1\cdots k_lk$, $kk_1\cdots k_l$, respectively.

By (22), $\Theta_{\phi\,;ij\,;\mathcal{K}_{l-1}}$ are symmetric with respect to the indexes $k_1,\cdots,k_{l-1}$, and it is easy to see, by induction on l, that

$$\Theta_{\phi\,;i,j\,;\mathcal{K}_{l-1}}=\sum_{\lambda=1}^{m}(A_{\phi\,;i\lambda}u^\lambda{}_{j\mathcal{K}_{l-1}}-A_{\phi\,;j\lambda}u^\lambda{}_{i\mathcal{K}_{l-1}})+B_{\phi\,;ij\,;\mathcal{K}_{l-1}} \tag{27}$$

where $B_{\phi;ij;\mathscr{K}_{l-1}}$ are analytic functions on $\mathscr{R}_{l_1}$ for $l_1 \geqq l-1$. Therefore it follows that $B_{\phi;ij;\mathscr{K}_{l-1}}$ are symmetric with respect to the indexes $k_1, \cdots, k_{l-1}$. $B_{\phi;ij;\mathscr{K}_{l-1}}$ are defined inductively by the formula:

$$(28)\quad B_{\phi;ij;k_1\cdots k_{l-1}} = \sum_{\lambda=1}^{m} \{(D_{k_{l-1}} \cdot A_{\phi;i\lambda}) \cdot u^{\lambda}{}_{jk_1\cdots k_{l-2}} \\ - (D_{k_{l-1}} \cdot A_{\phi;j\lambda}) \cdot u^{\lambda}{}_{ik_1\cdots k_{l-2}}\} + D_{k_{l-2}} \cdot B_{\phi;ij:k_1\cdots k_{l-2}},$$

$(l \geqq 2)$, where, when $l-1=0$, $B_{\phi;ij:k_1\cdots k_{l-1}}$ means $B_{\phi;ij}$.

Let $\mathscr{R}_l{}^{[0]}\Sigma$ be the ideal of $\Lambda^0\mathscr{R}_l$ generated by all $\Theta_{\phi;ij;\mathscr{K}_\nu}$ $(i, j, k_1, \cdots, k_\nu = 1, \cdots, p;\ \nu = 0, 1, \cdots, l-1;\ \phi \in \Sigma^{[2]})$. Since $\Sigma^{[2]}$ is finitely generated, $\mathscr{R}_l{}^{[0]}\Sigma$ is also finitely generated.

Definition II.2. Let $\mathscr{R}_l\Sigma$ be the exterior differential system on $\mathscr{R}_l$ generated by Π_l and $\mathscr{R}_l{}^{[0]}\Sigma$, for $l \geqq 1$.

Set $\mathscr{R}_0\Sigma = \Sigma$ on $\mathfrak{V}$. It is easy to prove the following relations:

$$(29)_l \qquad \text{if } 0 \leqq \nu \leqq l-2,\ d\Theta_{\phi;ij;\mathscr{K}_\nu} \equiv \sum_{k=1}^{p} \Theta_{\phi;ij;\mathscr{K}_\nu k}\omega^k \quad (\text{mod.}\ \pi_l),$$

$$(30)_l \quad d\Theta_{\phi;ij;\mathscr{K}_{l-1}} \equiv \sum_{\lambda=1}^{m} (A_{\phi;i\lambda}\, du^{\lambda}{}_{j\mathscr{K}_{l-1}} - A_{\phi;j\lambda} du^{\lambda}{}_{i\mathscr{K}_{l-1}}) + \sum_{k=1}^{p} B_{\phi;ij;\mathscr{K}_{l-1}k},$$

$$(31)_l \qquad d\theta^{\alpha} \equiv 0 \quad \text{mod}\{\Theta_{\phi;ij;};\ \phi \in \Sigma^{[2]}, i, j = 1, \cdots, p\},$$

$$(32)_l \qquad d^*\varpi^{\lambda}{}_{\mathscr{K}_\nu} = \sum_{k=1}^{p} {}^*\varpi^{\lambda}{}_{\mathscr{K}_\nu k} \wedge \omega^k.$$

THEOREM II.2. *$(\mathscr{R}_l\Sigma, \Omega)$ on $\mathscr{R}_l$ is isomorphic to an admissible restriction of $\mathscr{P}^l(\Sigma, \Omega)$ $(l = 0, 1, \cdots)$. The character c_l of the restriction is equal to $\sum_{\nu=0}^{l-1} (p+1)^{l-1-\nu} c_\nu'$, where $c_0' = \alpha_1 p$ and*

$$c_\nu' = \alpha_1 p + \tfrac{1}{2}mp(p-1)(C_{\nu-1}{}^{p+\nu-2}) + \sum_{h=1}^{\nu-1} (C_h{}^{p+h-1}) \quad \text{for } \nu \geqq 1.$$

Proof. (Induction on l). In the case $l = 0$, the theorem is trivial. Assuming that the theorem holds for l, we shall prove it for $l+1$. The proof for the case $l+1=1$ is almost the same as that for the case $l+1>1$ and is easier. Therefore we shall deal with the case $l+1>1$. By Propositions II.2 and II.3, it is sufficient to show that $(\mathscr{R}_{l+1}\Sigma, \Omega)$ is isomorphic to an admissible restriction of $\mathscr{P}(\mathscr{R}_l\Sigma, \Omega)$ of the character c_l'.

$\omega^1, \cdots, \omega^p$, $(\Pi_l), \cdots, du^{\lambda}{}_{k_1\cdots k_l}$ form a base of Pfaffian forms on $\mathscr{R}_l$. Hence as in **4** of Preliminaries, $\mathscr{G}_\Omega(\mathscr{R}_l, p) = \mathscr{G}(\mathscr{R}_l, p)$ has a system of coordinates $x^1, \cdots, x^n, \cdots, u^{\lambda}{}_{k_1\cdots k_\nu}, \cdots,$ $(\nu = 1, \cdots, l)$,

$$v_k{}^{\alpha}, v^{\lambda}{}_{;k}, \cdots, v^{\lambda}{}_{\mathscr{K}_\nu:k}, \cdots, v^{\lambda}{}_{\mathscr{K}_{l-1};k}, w^{\lambda}{}_{\mathscr{K}_l:k}$$

p14917

defined as follows: (i) $x^1, \cdots, x^n$ is a system of coordinates on $\mathfrak{V}$, (ii) if E is in $\mathfrak{G}(\mathcal{R}_l, p)$, E is the space of all solutions of the following system of linear equations on the tangent vector space to $\mathcal{R}_l$ at the origin of E:

$$\theta^\alpha - \sum_{k=1}^{p} v_k{}^\alpha(E)\,\omega^k = 0,$$

$$(33)\qquad {}^*\varpi^\lambda - \sum_{k=1}^{p} v^\lambda{}_{;k}(E)\,\omega^k = 0, \qquad {}^*\varpi^\lambda{}_{k_1} - \sum_{k=1}^{p} v^\lambda{}_{k_1;k}(E)\,\omega^k = 0, \cdots,$$

$$ {}^*\varpi^\lambda{}_{\mathfrak{K}_{l-1}} - \sum_{k=1}^{p} v^\lambda{}_{\mathfrak{K}_{l-1};k}(E)\,\omega^k = 0, \qquad du^\lambda{}_{\mathfrak{K}_l} - \sum_{k=1}^{p} w^\lambda{}_{\mathfrak{K}_l;k}(E)\,\omega^k = 0.$$

To avoid confusion, let Ω_l be the system of independent variables Ω on $\mathcal{R}_l$ and ρ_l be the projection $\mathfrak{G}(\mathcal{R}_l, p) \to \mathcal{R}_l$. Then, by Proposition I. 8, $\Pi^{[1]}\Omega_l$ is generated by

$$(34)\qquad \theta^\alpha - \sum_{k=1}^{p} v_k{}^\alpha\omega^k, \qquad {}^*\varpi^\lambda - \sum_{k=1}^{p} v^\lambda{}_{;k}\omega^k, \qquad {}^*\varpi^\lambda{}_{k_1} - \sum_{k=1}^{p} v^\lambda{}_{k_1;k}\omega^k, \cdots,$$

$$ {}^*\varpi^\lambda{}_{\mathfrak{K}_{l-1}} - \sum_{k=1}^{p} v^\lambda{}_{\mathfrak{K}_{l-1};k}\omega^k, \qquad du^\lambda{}_{\mathfrak{K}_l} - \sum_{k=1}^{p} w^\lambda{}_{\mathfrak{K}_l;k}\omega^k.$$

Then, by Definition I. 19 and Lemma I. 2, it follows that $(\mathfrak{P}\mathcal{R}_l\Sigma)^{[0]}$ is generated by

$$\Theta_{\phi;ij;\mathfrak{K}_\nu}, \ (\nu = 0, 1, \cdots, l-1; \phi \in \Sigma^{[2]}),$$

$$K[d\Theta_{\phi;ij;\mathfrak{K}_\nu}, p; k] \equiv \Theta_{\phi;ij;\mathfrak{K}_\nu k}, \ \mathrm{mod}(v^\lambda{}_{;k}, v^\lambda{}_{j_1;k}, \cdots, v^\lambda{}_{j_1\cdots j_{l-1};k}), \ (\text{cf. } (29)_l),$$

$$K[d\Theta_{\phi;ij;\mathfrak{K}_{l-1}}, p; k] \equiv \sum_{\lambda=1}^{m} (A_{\phi;i\lambda} w^\lambda{}_{j\mathfrak{K}_{l-1};k}$$

$$- A_{\phi;j\lambda} w^\lambda{}_{i\mathfrak{K}_{l-1};k}) + B_{\phi;ij;\mathfrak{K}_{l-1}}, \ \mathrm{mod}(v^\lambda{}_{;k}, v^\lambda{}_{j_1;k}, \cdots, v^\lambda{}_{j_1\cdots j_{l-1};k}), \ (\text{cf. } (30)_l),$$

$$K_k{}^{\theta^\alpha} = v_k{}^\alpha, \ K[{}^*\varpi^\lambda, p; k] = v^\lambda{}_{;k},$$

$$K[{}^*\varpi^\lambda{}_{k_1}, p; k] = v^\lambda{}_{k_1;k}, \cdots, \ K[{}^*\varpi^\lambda{}_{\mathfrak{K}_{l-1}}, p; k] = v_{\mathfrak{K}_{l-1};k}$$

$$K[d{}^*\varpi^\lambda{}_{\mathfrak{K}_\nu}, p; i, j] \equiv 0 \ (\mathrm{mod}\, v^\lambda{}_{;k}, v^\lambda{}_{j_1;k}, \cdots, v^\lambda{}_{j_1\cdots j_{l-1};k}),$$

$$(\nu = 0, 1, \cdots, l-2; \text{ cf. } (32)_l),$$

$$K[d{}^*\varpi^\lambda{}_{\mathfrak{K}_{l-1}}, p; i, j] = w^\lambda{}_{\mathfrak{K}_{l-1}i;j} - w^\lambda{}_{\mathfrak{K}_{l-1}j;i}, \text{ and}$$

$$K[d\theta^\alpha, p; i, j] \equiv 0 \quad (\mathrm{mod}\, \Theta_{\phi;k_1k_2}).$$

Let Σ^* be the restriction of $\mathfrak{P}_\Omega\mathcal{R}_l\Sigma$ to the submanifold $\mathfrak{G}^*$ of $\mathfrak{G}(\mathcal{R}_l, p)$ defined by the equations:

$$(35)\qquad v_k{}^\alpha = v^\lambda{}_{;k} = v^\lambda{}_{k_1;k} = \cdots = v^\lambda{}_{\mathfrak{K}_{l-1};k} = w^\lambda{}_{\mathfrak{K}_{l-1}i;j} - w^\lambda{}_{\mathfrak{K}_{l-1}j;i} = 0$$

$$(\alpha = 1, \cdots, \alpha_1; \lambda = 1, \cdots, m; i, j, k, k_1, \cdots, k_{l-1} = 1, \cdots, p).$$

Then Σ^* is an admissible restriction of $\mathcal{P}_\Omega \mathcal{R}_l \Sigma$ of character c_l' and $\Sigma^{*[0]}$ is generated by all $\Theta_{\phi\,;ij\,;}, \Theta_{\phi\,;ij\,;k_1}, \cdots, \Theta_{\phi\,;ij\,;\mathcal{K}_{l-1}}$, and by

$$\sum_{\lambda=1}^{m} (A_{\phi\,;i\lambda} w^\lambda{}_{j\mathcal{K}_{l-1};k} - A_{\phi\,;j\lambda} w^\lambda{}_{i\mathcal{K}_{l-1};k}) + B_{\phi\,;ij\,;\mathcal{K}_{l-1}k}.$$

$\Sigma^{*[1]}$ is generated by $d\Sigma^{*[0]}$, by θ^a, ${}^*\varpi^\lambda$, ${}^*\varpi^\lambda{}_{k_1}, \cdots, {}^*\varpi_{\mathcal{K}_{l-1}}$, and by $du^\lambda{}_{\mathcal{K}_{l-1}} - \sum_{k=1}^{p} w^\lambda{}_{\mathcal{K}_{l-1};k} \omega^k$. Σ^* is generated by $\Sigma^{*[0]}$, $\Sigma^{*[1]}$, and $d\Sigma^{[1]}$. Then it is clear that the mapping $\mathcal{R}_{l+1} \to \mathcal{G}^*$, defined by $u^\lambda{}_{k_1 \cdots k_{l+1}} \to w^\lambda{}_{k_1 \cdots k_l\,;k_{l+1}}$ and by $\mathcal{R}_l \to \mathcal{R}_l$ (identity mapping), is well defined and induces an isomorphism from $(\mathcal{R}_{l+1}\Sigma, \Omega)$ onto $(\mathcal{G}^*, \Omega)$. The number of independent equations in (35) is equal to c_l'. Thus the proof of Theorem II. 2 is completed.

4. System of polar forms of $\mathcal{R}_l\Sigma$. Let us make explicit the system of polar forms $J(E)$ of an integral element E of $(\mathcal{R}_l\Sigma, \Omega)$. Let ρ_q be the projection of $\mathcal{G}(\mathcal{R}_l, q) = \mathcal{G}_\Omega(\mathcal{R}_l, q)$ onto $\mathcal{R}_l$. We shall omit $\circ \rho_q$ and ρ_q^* in $A_{\phi\,;i\lambda} \circ \rho_q$, $\rho_q^* \omega^i$, etc., since the omission will not cause any confusion. Note that $\omega^1, \cdots, \omega^p, \theta^1, \cdots, \theta^{a_1}, \varpi^1, \cdots, \varpi^m$ is the base of Pfaffian forms on $\mathcal{V}$ fixed at the beginning of § 3.

(36) $\mathcal{V}_l^q = \{E \in \mathcal{G}(\mathcal{R}_l, q)\,;\, \omega^1, \cdots, \omega^q$ are linearly independent on $E\}$.

$\mathcal{V}_l^q$ is an open submanifold of $\mathcal{G}(\mathcal{R}_l, q)$ and $\mathcal{V}_l^p = \mathcal{G}(\mathcal{R}_l, p)$. Define the tangent vectors $L_1(E), \cdots, L_q(E)$ to $\mathcal{R}_l$, contained in E, by the formulas:

(37) $\langle \omega^{r'}, L_r(E) \rangle = \delta_r^{r'} \qquad (r', r = 1, \cdots, q),$

for any E in $\mathcal{V}_l^q$. Denote by η_q the projection of $\mathcal{V}_l^q$ onto $\mathcal{V}_l^{q-1}$ defined by the formula

(38) $\eta_q(E) = \{$the space spanned by $L_1(E), \cdots, L_{q-1}(E)\}$,

$(E \in \mathcal{V}_l^q)$. η_q is defined for $q = 1, \cdots, p$. Define analytic functions $w_r{}^{q,h}$ and $w^{q,\lambda}{}_{\mathcal{K}_l\,;r}$ on $\mathcal{V}_l^q$ by the formula:

(39) $w_r{}^{q,h}(E) = \langle \omega^{q+h}, L_r(E) \rangle, \qquad w^{q,\lambda}{}_{\mathcal{K}_l\,;r}(E) = \langle du^\lambda{}_{\mathcal{K}_l}, L_r(E) \rangle,$

$(E \in \mathcal{V}_q{}^l\,;\, r = 1, \cdots, q\,;\, h = 1, \cdots, p - q\,;\, \lambda = 1, \cdots, m\,;\, k_1 \cdots k_l = 1, \cdots, p).$

Clearly we have

(40) $w_r{}^{q-1,h+1} \circ \eta_q = w_r{}^{q,h}, \qquad$ (41) $w^{q-1,\lambda}{}_{\mathcal{K}_l\,;r} \circ \eta_q = w^{q,\lambda}{}_{\mathcal{K}_l\,;r},$

for $r = 1, \cdots, q - 1$. Denote by $\rho_q^* \cdot \Lambda^1 \mathcal{R}_l$ the $\Lambda^c \mathcal{V}_l^q$-submodule of $\Lambda^1 \mathcal{V}_l^q$ generated by all $\rho_q^* \cdot \theta, \theta \in \Lambda^1 \mathcal{R}_l$.

Definition II. 3. Denote by $\boldsymbol{A}_l^q$ the $\Lambda^0\mathfrak{V}_l^q$-submodule of $\rho_q^* \cdot \Lambda^1 \mathcal{R}_l$ generated by the following set of Pfaffian forms defined on $\mathfrak{V}_q^l$:

$$\xi_{\phi\,;ij\,;\,\mathcal{K}_{l-1}} = \sum_{\lambda=1}^{m} (A_{\phi\,;i\lambda} du^\lambda{}_{j\,\mathcal{K}_{l-1}} - A_{\phi\,;j\lambda} du^\lambda{}_{i\,\mathcal{K}_{l-1}}) + \sum_{k=1}^{p} B_{\phi\,;ij\,;\,\mathcal{K}_{l-1}k}\,\omega^k,$$

$$(\boldsymbol{A}_l^q) \qquad \zeta^\lambda{}_{\mathcal{K}_{l-1};r} = du^\lambda{}_{\mathcal{K}_{l-1}r} + \sum_{h=1}^{p-q} w_r^{q,h}\, du^\lambda{}_{\mathcal{K}_{l-1}q+h} - \sum_{k=1}^{p} w^{q,\lambda}{}_{\mathcal{K}_{l-1}k\,;r} \cdot \omega^k$$

$$(\phi \in \Sigma^{[2]};\ i, j, k_1, \cdots, k_{l-1} = 1, \cdots, p;\ \lambda = 1, \cdots, m;\ r = 1, \cdots, q).$$

We remark that $\boldsymbol{A}_l^0$ is the submodule generated by all $\xi_{\phi\,;ij\,;\,\mathcal{K}_{l-1}}$. According to the notations in § 5 of Chapter I, if

$$\xi = f_1 \cdot \rho_q^*\theta_1 + \cdots + f_a \cdot \rho_q^*\theta_a,$$
$$(f_1, \cdots, f_a \in \Lambda^0\mathfrak{V}_l^q, \theta_1, \cdots, \theta_a \in \Lambda^1\mathcal{R}_l),$$

and if E is in $\mathfrak{V}_l^q$, then $\langle \xi, \mathcal{E}_y\mathcal{R}_l \rangle_E$, where y is the origin of E, is the linear functional on the tangent vector space $\mathcal{E}_y\mathcal{R}_l$ to $\mathcal{R}_l$ at y, defined by the formula: $\langle \xi, \mathcal{E}_y\mathcal{R}_l \rangle_E = f_1(E) \cdot \langle \theta_1, \mathcal{E}_y\mathcal{R}_l \rangle + \cdots + f_a(E) \cdot \langle \theta_a, \mathcal{E}_y\mathcal{R}_l \rangle$. Then we have the following

Proposition II. 4. If E is in $\mathfrak{V}_q^l$ and if the origin $y = \rho_q(E)$ is an integral point of $\mathcal{R}_l\Sigma$, then

$$J(E) = \langle \pi_l, \mathcal{E}_y\mathcal{R}_l \rangle + \langle \boldsymbol{A}_l^q, \mathcal{E}_y\mathcal{R}_l \rangle_E,$$

where the plus sign denotes the direct sum.

Proof. By the definition of $J(E)$, (Definition I. 6), it is generated by the following linear functionals on $\mathcal{E}_y\mathcal{R}_l$:

$$(42)_\nu \qquad \langle d\Theta_{\phi\,;ij\,;\,\mathcal{K}_\nu}, \mathcal{E}_y\mathcal{R}_l \rangle$$

for $\nu = 0, 1, \cdots, l-1$,

$$(43) \qquad \langle \Pi_l, \mathcal{E}_y\mathcal{R}_l \rangle,$$

$$(44) \qquad d\theta^\alpha[L_r(E)], \text{ and } d^*\varpi^\lambda{}_{\mathcal{K}_\nu}[L_r(E)], \qquad (\nu = 0, 1, \cdots, l-1).$$

(cf. (10)). Since y is an integral point of $\mathcal{R}_l\Sigma$, $(29)_l$ implies that the members in $(42)_\nu$ are congruent to 0 modulo (43) for $\nu = 0, 1, \cdots, l-2$. $(30)_l$ implies that

$$\langle d\Theta_{\phi\,;ij\,;\,\mathcal{K}_{l-1}}, \mathcal{E}_y\mathcal{R}_l \rangle \equiv \langle \xi_{\phi\,;ij\,;\,\mathcal{K}_{l-1}}, \mathcal{E}_y\mathcal{R}_l \rangle_E$$

modulo $\langle \pi_l, \mathcal{E}_y\mathcal{R}_l \rangle$. By $(31)_l$ and $(32)_l$, members in (44) are congruent to 0 modulo (43) except $d^*\varpi^\lambda{}_{k_1\cdots k_{l-1}}[L_r(E)]$. A direct calculation shows that

$$-d^*\varpi^\lambda{}_{\mathcal{K}_{l-1}}[L_r(E)] = \langle \zeta^\lambda{}_{\mathcal{K}_{l-1};r}, \mathcal{E}_y\mathcal{R}_l \rangle_E.$$

Hence $J(E)$ is generated by $\langle \Pi_l, \mathcal{E}_y \mathcal{R}_l \rangle$ and $\langle A_l{}^q, \mathcal{E}_y \mathcal{R}_l \rangle_E$. Since ${}^*\varpi^\lambda{}_{\mathcal{K}_\nu}$ $(\nu = 0, 1, \cdots, l-1)$, $\omega^1, \cdots, \omega^p$, $du_{\mathcal{K}_l}$ form a base of Pfaffian forms on $\mathcal{R}_l$, we see easily, by the explicit expressions for the members in (Π_l) and $(\boldsymbol{A}_l{}^q)$, that the summation must be a direct sum.

Proposition II. 5. Let $\boldsymbol{A}_l(q)$, $p \geqq q \geqq 1$, be the $\Lambda^0 \mathfrak{V}_l{}^q$-submodule of $\rho_q{}^* \Lambda^1 \mathcal{R}_l$ generated by all $\zeta^\lambda{}_{k_1 \cdots k_{l-1};q}$. Let E be an element in $\mathfrak{V}_l{}^q$ whose origin y is an integral point of $\mathcal{R}_l \Sigma$. Set $E' = \eta_q(E)$. Then $\langle \boldsymbol{A}_l{}^q, \mathcal{E}_y \mathcal{R}_1 \rangle_E$ is generated by $\langle \boldsymbol{A}_l{}^{i-1}, \mathcal{E}_y \mathcal{R}_l \rangle_{E'}$ and $\langle \boldsymbol{A}_l(q), \mathcal{E}_y \mathcal{R}_l \rangle_E$.

Proof. Clearly $L_r(E') = L_r(E)$ for $r = 1, \cdots, q-1$. Then the proposition follows from the definition of $\boldsymbol{A}_l{}^q$, (40), and from (41).

In the following, we shall write $\mathcal{K}$ instead of $\mathcal{K}_{l-1}$.

Definition II. 4. Denote by $\boldsymbol{A}'_l{}^q$ the $\Lambda^0 \mathfrak{V}_l{}^q$-submodule of $\rho_q{}^* \cdot \Lambda^1 \mathcal{R}_l$ generated by the following set of Pfaffian forms defined on $\mathfrak{V}_l{}^q$.

$$(\boldsymbol{A}'_l{}^q) \qquad \begin{aligned} \xi'_{\phi;ij;\mathcal{K}} &= \sum_{\lambda=1}^{m} (A_{\phi;i\lambda} du^\lambda{}_{j\mathcal{K}} - A_{\phi;j\lambda} du^\lambda{}_{i\mathcal{K}}), \\ \zeta'^\lambda{}_{\mathcal{K};r} &= du_{\mathcal{K}r} + \sum_{h=1}^{p-q} w_r{}^{q,h} du_{\mathcal{K}\, q+h}; \end{aligned}$$

$$(\phi \in \Sigma^{[2]};\ \lambda = 1, \cdots, m;\ r = 1, \cdots, q;\ i, j, k_1, \cdots, k_{l-1} = 1, \cdots, p).$$

Set

$$(45) \qquad t'(E) = \dim \langle \boldsymbol{A}'_l{}^q, \mathcal{E}_y \mathcal{R}_l \rangle_E, \qquad (y = \text{the origin of } E, E \in \mathfrak{V}_l{}^q).$$

Then by Proposition II. 4 we have the formula

$$(45)' \quad \dim(J(E) \bmod \langle \Omega, \mathcal{E}_y \mathcal{R}_l \rangle) = t'(E) + n - p + m(\sum_{\nu=1}^{l-1} C_\nu{}^{p+\nu-1}).$$

Proposition II. 6. Let E be a q-dimensional integral element of $\mathcal{R}_l \Sigma$. Assume that E is $\mathfrak{V}_l{}^q$. Set $E' = \eta_q(E)$ (cf. (38)), and $E'' = d\rho_{l-1}{}^l \cdot E'$, where $\rho_{l-1}{}^l$ is the projection $\mathcal{R}_l \to \mathcal{R}_{l-1}$. Let y be the origin of E. Then

$$t'(E) \leqq \dim \langle \boldsymbol{A}_l{}^q, \mathcal{E}_y \mathcal{R}_l \rangle_E \leqq \dim \langle \boldsymbol{A}_l{}^{q-1}, \mathcal{E}_y \mathcal{R}_l \rangle_{E'} + n_{l-1} - t'(E''),$$

where $n_{l-1} = \dim \mathcal{R}_{l-1} = m \cdot C_{l-1}{}^{p+l-2}$.

To simplify the notations we shall omit $\langle\ , \mathcal{E}_y \mathcal{R}_l \rangle$ and $\langle\ , \mathcal{E}_y \mathcal{R}_l \rangle_E$. Thus, for example, $du^\lambda{}_{\mathcal{K}}$ and $\zeta^\lambda{}_{\mathcal{K};r}$ means $\langle du^\lambda{}_{\mathcal{K}}, \mathcal{E}_y \mathcal{R}_l \rangle$ and $\langle \zeta^\lambda{}_{\mathcal{K};r}, \mathcal{E}_y \mathcal{R}_l \rangle_E$, respectively. In general, we shall denote by $\mathcal{H}$ the set of indexes $k_1, \cdots, k_{l-2}$. As before, $\mathcal{K}$ represents the set of indexes $k_1, \cdots, k_{l-1}$. Let $du_{\mathcal{K}_\chi}{}^{\lambda_\chi}$, $(\chi \in \mathrm{X})$, be the maximal number independent $du_{\mathcal{K}}{}^\lambda \bmod \langle \boldsymbol{A}'_{l-1}{}^{q-1}, \mathcal{E}_{y'} \mathcal{R}_{l-1} \rangle_{E''} \circ d\rho_{l-1}{}^l$, where $y' = \rho_{l-1}{}^l(y)$ and X is a set of indexes. Then the number of elements in X is $n_{l-1}-t'(E'')$. Take any λ and $\mathcal{K}$. Then, adopting the tensor notations, we can write

$$du^{\lambda}{}_{\mathcal{K}}=a_{\chi}du^{\lambda\chi}{}_{\mathcal{K}\chi}+b^{\phi;ij;\mathfrak{H}}\xi'_{\phi;ij;\mathfrak{H}}\circ d\rho^{l}{}_{l-1}+c_{\lambda}{}^{\mathfrak{H};r'}\zeta'^{\lambda}{}_{\mathfrak{H};r'}\circ d\rho^{l}{}_{l-1},$$

$(r'=1,\cdots,q-1)$, where a_{χ}, $b^{\phi;ij;\mathfrak{H}}$, $c_{\lambda}{}^{\mathfrak{H};r'}$ are constants. We claim that, for any $k=1,\cdots,p$,

$$\text{(a)}\qquad du^{\lambda}{}_{\mathcal{K}k}=a_{\chi}du^{\lambda\chi}{}_{\mathcal{K}\chi k}+b^{\phi;ij;\mathfrak{H}}\xi'_{\phi;ij;\mathfrak{H}k}+c_{\lambda}{}^{\mathfrak{H};r'}\zeta'_{\mathfrak{H}k;r'}.$$

To prove formula (a), observe that, for each k, there is an isomorphism of the space generated by $\langle du^{\lambda}{}_{\mathfrak{H}},\mathcal{E}_{y'}(\mathcal{R}^{l-1})\rangle$ which maps each $du^{\lambda}{}_{\mathfrak{H}}$ upon $du^{\lambda}{}_{\mathfrak{H}k}$. Then clearly this mapping maps $\xi'_{\phi;ij;\mathfrak{H}}$ upon $\xi'_{\phi;ij;\mathfrak{H}k}$. Since $w_{r}{}^{q,h}(E)=w_{r}{}^{q,h}(\rho^{l}{}_{l-1}(E))$ by (39), it follows that this mapping maps $\zeta'^{\lambda}{}_{\mathfrak{H};r'}$ upon $\zeta'^{\lambda}{}_{\mathfrak{H}k;r'}$. Therefore formula (a) holds.

Since E is an integral element of $\mathcal{R}_{l}\Sigma$, taking the value at $L_{q}(E)$, we have the equality

$$\begin{aligned}\text{(b)}\quad w^{q,\lambda}{}_{\mathcal{K}k;q}(E)=a_{\chi}w^{q,\lambda\chi}{}_{\mathcal{K}\chi k;q}(E)&-b^{\phi;ij;\mathfrak{H}}(B_{\phi;ij;\mathfrak{H}kq}(y)\\&+w_{q}{}^{q,h}(E)B_{\phi;ij;\mathfrak{H}kq+h}(y))+c_{\lambda}{}^{\mathfrak{H};r'}(w^{q,\lambda}{}_{\mathfrak{H}kq;r'}(E)\\&\qquad+w_{q}{}^{q,h}(E)w^{q,\lambda}{}_{\mathfrak{H}kq+h;r'}(E)).\end{aligned}$$

Then, by (a) and (b),

$$\begin{aligned}\zeta^{\lambda}{}_{\mathcal{K};q}&=du^{\lambda}{}_{\mathcal{K}q}+w_{q}{}^{q,h}(E)du^{\lambda}{}_{\mathcal{K}q+h}-w^{q,\lambda}{}_{\mathcal{K}k;q}(E)\omega^{k}\\&=a_{\chi}\zeta^{\lambda\chi}{}_{\mathcal{K}\chi;q}+b^{\phi;ij;\mathfrak{H}}(\xi_{\phi;ij;\mathfrak{H}q}+w_{q}{}^{q,h}(E)\xi_{\phi;ij;\mathfrak{H}q+h})\\&\qquad+c_{\lambda}{}^{\mathfrak{H};r'}(\zeta^{\lambda}{}_{\mathfrak{H}q;r'}+w_{q}{}^{q,h}(E)\xi^{\lambda}{}_{\mathfrak{H}q+h;r'}),\end{aligned}$$

since $B_{\phi;ij;k_1\cdots k_l}$ and $w^{q,\lambda}{}_{k_1\cdots k_l;r}$ are symmetric with respect to the indexes $k_1,\cdots,k_l$. Therefore

$$\zeta^{\lambda}{}_{\mathcal{K};q}\equiv a_{\chi}\zeta^{\lambda\chi}{}_{\mathcal{K}\chi;q}\ (\operatorname{mod}\langle A_{l}{}^{q-1},\mathcal{E}_{y}\mathcal{R}_{l}\rangle_{E'}\circ d\rho^{l}{}_{l-1}).$$

Then, by Proposition II. 5,

$$\begin{aligned}\dim\langle A_{l}{}^{q},\mathcal{E}_{y}\mathcal{R}_{l}\rangle_{E}&\leqq\dim\langle A_{l}{}^{q-1},\mathcal{E}_{y}\mathcal{R}_{l}\rangle_{E'}+\text{the number of indexes in X}\\&=\dim\langle A_{l}{}^{q-1},\mathcal{E}_{y}\mathcal{R}_{l}\rangle_{E'}+n_{l-1}-t'(E'').\end{aligned}$$

Chapter III. Prolongation Theorem.

The problem we are going to concern ourselves with is the following: when the given normal system (Σ, Ω) is not involutive (Definition I. 17), what are the conditions that will assure the involutiveness of the l-th prolongation $\mathcal{P}^l(\Sigma, \Omega)$ of (Σ, Ω) for sufficiently large l? By Theorem II. 2, it is sufficient, for that purpose, to examine $(\mathcal{R}_l\Sigma, \Omega)$. We shall first study the ranks of the reduced polar equations of integral elements, which are equal to the dimensions of the $A'_l{}^q$. The Definition II. 4 suggests that they may be equal to the dimensions of homogeneous parts of appropriately defined ideals in some polynomial rings. This will be done in § **1** and § **2**. Then, using the Noetherian property of polynomial ring, we shall derive, in § **3**, the crucial property of the reduced characters, which will help, with Proposition II. 6, to bridge the characters and the reduced characters (§ **5**). To complete this bridge, we must choose points which are regular in some respects (§ **4**), and the differential system must satisfy some conditions. The exact form of the conditions will be given in the fundamental theorem in § **6**. These conditions are also necessary for $\mathcal{P}^l(\Sigma, \Omega)$ to be involutive. In § 7, we shall give an example which indicates that our conditions are, in some respect, the best possible one.

1. Fiber bundles associated with a system of independent variables. Let Ω be a system of p independent variables on $\mathcal{V}$. For any point x of $\mathcal{V}$, denote by $\mathcal{E}^*{}_x\mathcal{V}$ the space of all tangent vectors L to $\mathcal{V}$ at x such that $\langle \omega, L \rangle = 0$ for all $\omega \in \Omega$. Set $\mathcal{E}^\dagger{}_x\mathcal{V} = \mathcal{E}_x\mathcal{V}/\mathcal{E}^*{}_x\mathcal{V}$. It is a p-dimensional space. The elements in $\mathcal{E}^\dagger{}_x\mathcal{V}$ will be called a reduced tangent vector to $\mathcal{V}$ at x (with respect to Ω). It is clear that $\mathcal{E}^\dagger\mathcal{V} = \bigcup \{\mathcal{E}^\dagger{}_x\mathcal{V}; x \in \mathcal{V}\}$ has a natural analytic manifold structure and is a fiber bundle over $\mathcal{V}$ with fiber $\mathcal{E}^\dagger{}_x\mathcal{V}$. Denote by $\rho^\dagger$ the projection. A q dimensional subspace $E^\dagger$ of $\mathcal{E}^\dagger{}_x\mathcal{V}$ will be called a reduced contact element to $\mathcal{V}$ at x (with respect to Ω), and x its origin. If $\omega \in \Omega$, we can naturally define $\langle \omega, E^\dagger \rangle$ as a linear functional on $E^\dagger$. The set of all q dimensional reduced contact elements forms an analytic manifold $\mathcal{G}^\dagger(\mathcal{V}, q)$. It is a fiber bundle with the base manifold $\mathcal{V}$ and with the projection $\rho^\dagger{}_q$, mapping each element to its origin. In particular, we shall identify $\mathcal{G}^\dagger(\mathcal{V}, 0)$ with $\mathcal{V}$.

We shall construct a system of coordinates on $\mathcal{G}^\dagger(\mathcal{V}, q)$. Let $\omega^1, \cdots, \omega^q$ be linearly independent elements in Ω. Set

$$(5)^\dagger \quad \mathcal{U}^\dagger(\omega^1, \cdots, \omega^q) = \{E^\dagger \in \mathcal{G}^\dagger(\mathcal{V}, q); \langle \omega^1, E^\dagger \rangle, \cdots, \langle \omega^q, E^\dagger \rangle \text{ are linearly independent}\}.$$

Let $L_r(E^\dagger)$ $(r=1,\cdots,q)$, be the elements in $E^\dagger$ defined by the formula

$$(6)^\dagger \qquad \langle \omega^{r'}, L_r(E^\dagger)\rangle = \delta_r{}^{r'}, \qquad (r, r'=1,\cdots,q)$$

Define the functions ${}^q w_r{}^h$, $(r=1,\cdots q; h=1,\cdots,p-q)$, on $\mathcal{U}^\dagger(\omega^1,\cdots,\omega^q)$ by the formula

$$(46) \qquad {}^q w_r{}^h(E^\dagger) = \langle w^{q+h}, L_r(E^\dagger)\rangle, \qquad (E^\dagger \in \mathfrak{G}^\dagger(\mathcal{V},q)).$$

If $(x_1,\cdots,x_n)$ is a system of coordinates on $\mathcal{V}$, then

$$(x_1 \circ \rho^\dagger{}_q, \cdots, x_n \circ \rho^\dagger{}_q, \cdots, {}^q w_r{}^h, \cdots)$$

is a system of coordinates on $\mathcal{U}^\dagger(\omega^1,\cdots,\omega^q)$.

In the remainder of the present paper, $(\omega^1,\cdots,\omega^p)$ represents a base of Ω. Then there is an analytic mapping $\eta^\dagger{}_q$ of $\mathcal{U}^\dagger(\omega^1,\cdots,\omega^q)$ onto $\mathcal{U}^\dagger(\omega^1,\cdots,\omega^{q-1})$ defined by the formula: for $E^\dagger \in \mathcal{U}^\dagger(\omega^1,\cdots,\omega^q)$

$$(47) \qquad \eta^\dagger{}_q(E^\dagger) = \text{the space spanned by } L_1(E^\dagger),\cdots,L_{q-1}(E^\dagger).$$

Then clearly

$$(48) \qquad {}^{q-1}w_r{}^{h+1} \circ \eta^\dagger{}_q = {}^q w_r{}^h \qquad (r=1,\cdots,q-1; h=1,\cdots,p-q).$$

Let $\mathcal{U}^\dagger$ be an open subset in $\mathfrak{G}^\dagger(\mathcal{V},q)$. By a cross-section of $\mathfrak{G}^\dagger(\mathcal{V},q)$ into $\mathcal{E}^\dagger\mathcal{V}$ over $\mathcal{U}^\dagger$, we mean an analytic mapping X of $\mathcal{U}^\dagger$ into $\mathcal{E}_x{}^\dagger\mathcal{V}$ such that $\rho^\dagger \circ X = \rho^\dagger{}_q$. Since $\mathcal{E}^\dagger{}_x\mathcal{V}$ is a module, it is clear that the set $\mathbf{X}^q(\mathcal{U}^\dagger,\Omega)$ of all cross-section of $\mathfrak{G}^\dagger(\mathcal{V},q)$ into $\mathcal{E}^\dagger\mathcal{V}$ over $\mathcal{U}^\dagger$ forms a module over the ring $\Lambda^0\mathcal{U}^\dagger$ of all analytic functions on $\mathcal{U}^\dagger$. If $\mathcal{U}^{\dagger\prime} \subset \mathcal{U}^\dagger$, the restrictions of cross-sections over $\mathcal{U}^\dagger$ to $\mathcal{U}^{\dagger\prime}$ induces an additive mapping ${}^\iota u^\dagger, u^{\dagger\prime}$: $\mathbf{X}^q(\mathcal{U},\Omega) \to \mathbf{X}^q(\mathcal{U}^{\dagger\prime},\Omega)$. If $\mathcal{U}^{\dagger\prime\prime} \subset \mathcal{U}^\dagger$, then clearly ${}^\iota u^{\dagger\prime}, u^{\dagger\prime\prime} \circ {}^\iota u^\dagger, u^{\dagger\prime} = {}^\iota u^\dagger, u^{\dagger\prime\prime}$. By the classical theorem of analytic functions, the mapping ${}^\iota u^\dagger, u^{\dagger\prime}$ is univalent. Denote by $X^q{}_i(\omega^1,\cdots,\omega^p)$ $(i=1,\cdots,q)$, the element in $X^q(\mathfrak{G}^\dagger(\mathcal{V},q),\Omega)$ defined by the formula

$$(49) \qquad [X^q{}_i(\omega^1,\cdots,\omega^p)](E^\dagger) = L_i(\mathcal{E}_x{}^\dagger\mathcal{V}), \quad (x=\rho_q(E^\dagger); E^\dagger \in \mathfrak{G}^\dagger(\mathcal{V},q))$$

Let $X^q{}_i(\omega^1,\cdots,\omega^p;\mathcal{U}^\dagger)$ be the restriction of $X^q{}_i(\omega^1,\cdots,\omega^p)$ to $\mathcal{U}^\dagger$. Then it is easy to see the following:

Proposition III. 1. Let $\mathcal{U}^\dagger$ be a connected open subset of $\mathfrak{G}^\dagger(\mathcal{V},q)$. Then the $\Lambda^0\mathcal{U}^\dagger$-module $\mathbf{X}^q(\mathcal{U},\Omega)$ is equal to the direct sum of the $\Lambda^0\mathcal{U}^\dagger \cdot \mathbf{X}^q{}_i$, $(i=1,\cdots,p)$, where $\mathbf{X}^q{}_i = \mathbf{X}^q{}_i\ (\omega^1,\cdots,\omega^p;\mathcal{U}^\dagger)$.

An element X in $\mathbf{X}^q(\mathcal{U}^\dagger,\Omega)$ is called proper, if $X(E^\dagger) \in E^\dagger$ for any $E^\dagger \in \mathcal{U}^\dagger$. Let $\mathfrak{X}^q(\mathcal{U}^\dagger,\Omega)$ be the set of all proper cross-section over $\mathcal{U}^\dagger$.

$\mathfrak{X}^q(\mathcal{U}^\dagger,\Omega)$ is a $\Lambda^0\mathcal{U}^\dagger$-submodule of $\boldsymbol{X}^q(\mathcal{U},\Omega)$. Suppose that $\mathcal{U}^\dagger\subseteq\mathcal{U}^\dagger(\omega^1,\cdots,\omega^q)$. Then

$$\mathcal{X}^q{}_r(\omega^1,\cdots,\omega^p;\mathcal{U}^\dagger)=X^q{}_r(\omega^1,\cdots,\omega^p,\mathcal{U}^\dagger)+\sum_{h=1}^{p-q}{}^qw_r{}^h\cdot X^q{}_{q+h}(\omega^1,\cdots,\omega^p;\mathcal{U}^\dagger)$$

is in $\mathfrak{X}^q(\mathcal{U}^\dagger,\Omega)$, where ${}^qw_r{}^h$ is the function defined by the formula (46).

Proposition III. 2. Let $\mathcal{U}^\dagger$ be a connected open set in $\mathcal{U}^\dagger(\omega^1,\cdots,\omega^q)$. Set $\mathcal{X}^q{}_r=\mathcal{X}^q{}_r(\omega^1,\cdots,\omega^p;\mathcal{U}^\dagger)$. Then $\Lambda^0\mathcal{U}^\dagger$-module $\mathfrak{X}^q(\mathcal{U}^\dagger,\Omega)$ is equal to the direct sum of the $\Lambda^0\mathcal{U}^\dagger\cdot\mathcal{X}^q{}_r$ $(r=1,\cdots,q)$.

For any manifold $\mathcal{V}$, let $[\Lambda^0]\mathcal{V}$ be the field of real meromorphic functions on $\mathcal{V}$. $[\Lambda^0]\mathcal{V}$ is equal to the field of quotient of $\Lambda^0\mathcal{V}$. Set $[\boldsymbol{X}^q](\mathcal{U}^\dagger,\Omega)=[\Lambda^0]\mathcal{U}^\dagger\underset{\Lambda^0\mathcal{U}^\dagger}{\otimes}\boldsymbol{X}^q(\mathcal{U}^\dagger,\Omega)$, the tensor product of $[\Lambda^0]\mathcal{U}^\dagger$ and $\boldsymbol{X}^q(\mathcal{U}^\dagger,\Omega)$ over $\Lambda^0\mathcal{U}^\dagger$. Set $[\mathfrak{X}^q](\mathcal{U}^\dagger,\Omega)=[\Lambda^0]\mathcal{U}^\dagger\underset{\Lambda^0\mathcal{U}^\dagger}{\otimes}\mathfrak{X}^q(\mathcal{U}^\dagger,\Omega)$. We can naturally identify $\boldsymbol{X}^q(\mathcal{U}^\dagger,\Omega)$ and $\mathfrak{X}^q(\mathcal{U}^\dagger,\Omega)$ with submodules of $[\boldsymbol{X}^q](\mathcal{U}^\dagger,\Omega)$ and $[\mathfrak{X}^q](\mathcal{U}^\dagger,\Omega)$, respectively. By Propositions III. 1 and III. 2, we have

Proposition III. 3. $[\boldsymbol{X}^q](\mathcal{U}^\dagger,\Omega)$ is a vector space over the field $[\Lambda^0]\mathcal{U}^\dagger$ of p dimensions. Then the $X_i(\omega^1,\cdots,\omega^p;\mathcal{U}^\dagger)$ $(i=1,\cdots,p)$, form a base of $[\boldsymbol{X}^q](\mathcal{U}^\dagger,\Omega)$. If, moreover, $\mathcal{U}^\dagger$ is contained in $\mathcal{U}^\dagger(\omega^1,\cdots,\omega^q)$, then $[\mathfrak{X}^q](\mathcal{U}^\dagger,\Omega)$ is a vector space over $[\Lambda^0]\mathcal{U}^\dagger$ of dimension q and the $\mathcal{X}_r{}^q(\omega^1,\cdots,\omega^1;\mathcal{U}^\dagger)$ $(r=1,\cdots,q)$, form a base of it.

2. Ideals associated with a normal system. Let (Σ,Ω) be a normal system over $\mathcal{V}$. Let p be the number of independent variables in Ω. For any subset Λ of $\Lambda^1\mathcal{V}$ and for any open subset $\mathcal{U}^\dagger$ of $\mathfrak{S}^\dagger(\mathcal{V},q)$, denote by $(\Lambda,\mathcal{U}^\dagger)$ the $\Lambda^0\mathcal{U}^\dagger$-submodule of $\Lambda^1\mathcal{U}^\dagger$ generated by all $\rho_q{}^{\dagger*}\theta$, $(\theta\in\Lambda)$. Set

$$Y^q(\Sigma,\mathcal{U}^\dagger)=(\Lambda^1\mathcal{V},\mathcal{U}^\dagger)/(\Sigma^{[1]}+\Omega,\mathcal{U}^\dagger) \tag{50}$$

$Y^q(\Sigma,\mathcal{U}^\dagger)$ is a module over the ring $\Lambda^0\mathcal{U}^\dagger$. If $\mathcal{U}^{\dagger\prime}\subseteq\mathcal{U}^\dagger$, there is an univalent additive mapping $\iota_{\mathcal{U}^\dagger,\mathcal{U}^{\dagger\prime}}$: $Y^q(\Sigma,\mathcal{U}^\dagger)\to Y^q(\Sigma,\mathcal{U}^{\dagger\prime})$. Set

$$[Y^q](\Sigma,\mathcal{U}^\dagger)=[\Lambda^0]\mathcal{U}^\dagger\underset{\Lambda^0\mathcal{U}^\dagger}{\otimes}Y^q(\Sigma,\mathcal{U}^\dagger).$$

$[Y^q](\Sigma,\mathcal{U}^\dagger)$ is a vector space over $[\Lambda^0]\mathcal{U}^\dagger$. By the condition (ii) of normal systems, one sees easily that $Y^q(\Sigma,\mathcal{U}^\dagger)$ is torsion free. Therefore we can naturally identity $Y^q(\Sigma,\mathcal{U}^\dagger)$ with a submodule of $[Y^q](\Sigma,\mathcal{U}^\dagger)$. For any ϖ in $\Lambda^1\mathcal{V}$, set

$$\{\varpi\}_q=\text{(the class modulo }(\Sigma^{[1]}+\Omega,\mathcal{U}^\dagger)\text{ containing }(\rho_q{}^\dagger)^*\varpi). \tag{51}$$

We remark that, by Definition II. 1, there is a base of $\Lambda^1\mathfrak{V}$-modulo $\Sigma^{[1]}+\Omega$. This base consists of m elements.

Proposition III. 4. $[\mathbf{Y}^q](\Sigma,\mathfrak{U}^\dagger)$ is a vector space of dimension m over $[\Lambda^0]\mathfrak{U}^\dagger$.

Let $\varpi^1,\cdots,\varpi^m$ be a base of $\Lambda^1\mathfrak{V}$ modulo $\Sigma^{[1]}+\Omega$. Then $\{\varpi^1\}_q,\cdots,\{\varpi^m\}_q$ form a base of $[\mathbf{Y}^q](\Sigma,\mathfrak{U}^\dagger)$. $\mathbf{Y}^q(\Sigma,\mathfrak{U}^\dagger)$ is equal to the direct sum of $\Lambda^0\mathfrak{U}^\dagger\cdot\{\varpi^\lambda\}_q$ $(\lambda=1,\cdots,m)$.

Denote by $[\mathbf{Z}](\Sigma,\mathfrak{U}^\dagger)$ the (abstract) direct sum of the vector space $[\mathbf{Y}^q](\Sigma,\mathfrak{U}^\dagger)+[\mathbf{X}^q](\mathfrak{U}^\dagger,\Omega)$. Let

$$\mathfrak{P}_q(\Sigma,\mathfrak{U}^\dagger) \tag{52}$$

be the symmetric algebra over $[\mathbf{Z}](\Sigma,\mathfrak{U}^\dagger)$. Thus if we choose bases $\omega^1,\cdots,\omega^p$ and $\varpi^1,\cdots,\varpi^m$ of Ω and of Λ^1V modulo $\Sigma^{[1]}+\Omega$, and if we set $X_i=X_i^q(\omega^1,\cdots,\omega^p;\mathfrak{U}^\dagger)$ and $Y^\lambda=\{\varpi^\lambda\}_q$, then the elements in $\mathfrak{P}_q(\Sigma,\mathfrak{U}^\dagger)$ are expressed as polynomials $X_1,\cdots,X_p$, $Y^1,\cdots,Y^m$ with coefficients in $[\Lambda^0]\mathfrak{U}^\dagger$. Let

$$\mathfrak{P}'_q(\Sigma,\mathfrak{U}^\dagger) \tag{53}$$

by the subring of $\mathfrak{P}_q(\Sigma,\mathfrak{U}^\dagger)$ which is $\Lambda^0\mathfrak{U}^\dagger$-generated by $\mathbf{Y}^q(\Sigma,\mathfrak{U}^\dagger)$ and $\mathbf{X}^q(\mathfrak{U}^\dagger,\Omega)$. Thus the elements in $\mathfrak{P}'_q(\Sigma,\mathfrak{U}^\dagger)$ are expressed as polynomials in $X_1,\cdots,X_p$, $Y^1,\cdots,Y^m$ with coefficients in $\Lambda^0\mathfrak{U}^\dagger$.

By Definition II. 1, we can write any $\phi\in\Sigma^{[2]}$ as

$$\phi\equiv\sum_{i=1}^{p}\sum_{\lambda=1}^{m}A_{\phi;ij}\omega^i\wedge\varpi^\lambda+\sum_{i=1}^{p}\sum_{j=1}^{p}\tfrac{1}{2}B_{\phi;ij}\omega^i\wedge\omega^j \quad (\operatorname{mod}\Sigma^{[1]}), \tag{24}$$

where $A_{\phi;i\lambda}$ and $B_{\phi;ij}$ are in $\Lambda^0\mathfrak{V}$ and $B_{\phi;ij}+B_{\phi;ji}=0$. Then

$$P_{\phi;ij}=\sum_{\lambda=1}^{m}(A_{\phi;i\lambda}\circ\rho_q^\dagger)\cdot Y^\lambda\cdot X_j-(A_{\phi;j\lambda}\circ\rho_q^\dagger)\cdot Y^\lambda\cdot X_i$$

is an element in $\mathfrak{P}'_q(\Sigma,\mathfrak{U}^\dagger)$. Of course, $P_{\phi;ij}$ depends on the choice of the bases $\omega^1,\cdots,\omega^p$ and $\varpi^1,\cdots,N^m$. But one can verify easily that the $\Lambda^0\mathfrak{U}^\dagger$-submodule $S_q(\mathfrak{U}^\dagger)$ of $P'_q(\Sigma,\mathfrak{U}^\dagger)$ generated by all $P_{\phi;ij}$, $(\phi\in\Sigma^{[2]})$, does not depend on the choice of the bases. Denote by $T_q(\mathfrak{U}^\dagger)$ the $\Lambda^0\mathfrak{U}^\dagger$-submodule of $\mathfrak{P}'_q(\Sigma,\mathfrak{U}^\dagger)$ generated by all $Y\cdot X$, where Y and X run through $\mathbf{Y}^q(\Sigma,\mathfrak{U}^\dagger)$ and $\mathrm{X}^q(\mathfrak{U}^\dagger,\Omega)$, respectively. When $q=0$, $T_q(\mathfrak{U}^\dagger)$ is defined to be 0.

Definition III. 1. $A_q(\Sigma,\mathfrak{U}^\dagger)$ is defined to be the ideal in $\mathfrak{P}_q(\Sigma,\mathfrak{U}^\dagger)$ generated by $S_q(\mathfrak{U}^\dagger)$ and $T_q(\mathfrak{U}^\dagger)$, $(q=0,1,\cdots,p-1)$. $A'_q(\Sigma,\mathfrak{U}^\dagger)$ is defined to be the ideal in $\mathfrak{P}'_q(\Sigma,\mathfrak{U}^\dagger)$ generated by $S_q(\mathfrak{U}^\dagger)$ and $T_q(\mathfrak{U}^\dagger)$.

Definition III. 2. $B_q(\Sigma, \mathcal{U}^\dagger)$ is defined to be the product of $Y^q(\Sigma, \mathcal{U}^\dagger)$ and $A^q(\Sigma, \mathcal{U}^\dagger)$. $B'_q(\Sigma, \mathcal{U}^\dagger)$ is defined to be the product of $Y^q(\Sigma, \mathcal{U}^\dagger)$ and $A'_q(\Sigma, \mathcal{U}^\dagger)$.

Proposition III. 5. Let $\mathcal{U}^\dagger$ be an open connected subset of $\mathcal{U}^\dagger(\omega^1, \cdots, \omega^q)$, (cf. $(5)^\dagger$). Set $X_i = X_i^q(\omega^1, \cdots, \omega^p; \mathcal{U}^\dagger)$. Let $\varpi^1, \cdots, \varpi^m$ be a base of $\Lambda^1\mathcal{V}$ modulo $\Sigma^{[1]} + \Omega$. Set $Y^\lambda = \{\varpi^\lambda\}_q$, (cf. (51)). Define the function ${}^q w_r{}^h$ on $\mathcal{U}^\dagger$ by the formula (46). Then $A_q(\Sigma, \mathcal{U}^\dagger)$ and $A'_q(\Sigma, \mathcal{U}^\dagger)$ are generated by all

$$\begin{aligned} \xi_{\phi\,;ij}(\mathcal{U}^\dagger) &= \sum_{\lambda=1}^{m} (A_{\phi\,;i\lambda} X_j - A_{\phi\,;j\lambda} X_i) Y^\lambda, \\ \zeta_r{}^\lambda(\mathcal{U}^\dagger) &= (X_r + \sum_{h=1}^{p-q} {}^q w_r{}^h \cdot X_{q+h}) Y^\lambda, \end{aligned} \tag{54}$$

$(\lambda = 1, \cdots, m; i, j = 1, \cdots, p; r = 1, \cdots, q)$ (cf. Proposition III. 2 and 3).

Let x be a point of $\mathcal{V}$. Set $Y(x) = \langle \Lambda^1\mathcal{V}, \mathcal{E}_x\mathcal{V}\rangle / \langle \Sigma^{[1]} + \Omega, \mathcal{E}_x\mathcal{V}\rangle$. Let

$$P(x) \tag{55}$$

be the symmetric algebra over the direct sum $Y(x) + \mathcal{E}^\dagger{}_x\mathcal{V}$. If we take bases $X_1, \cdots, X_p$, and $Y^1, \cdots, Y^m$ of $\mathcal{E}^\dagger{}_x\mathcal{V}$ and $Y(x)$, then $P(x)$ is canonically isomorphic to the polynomial ring $\boldsymbol{R}[X_1, \cdots, X_p, Y^1, \cdots, Y^m]$. Let $E^\dagger$ be a q dimensional reduced contact element to $\mathcal{V}$ at x. Then taking the value at $E^\dagger$, we can define, for any $E^\dagger \in \mathcal{U}^\dagger$, a homomorphism

$$\kappa_{E^\dagger} \colon \mathcal{P}'_q(\Sigma, \mathcal{U}^\dagger) \to P(x).$$

More explicitly, if one take bases $\omega^1, \cdots, \omega^p$ and $\varpi^1, \cdots, \varpi^m$ of Ω and of $\Lambda^1 V$ modulo $\Sigma^{[1]} + \Omega$, respectively, then $\kappa_{E^\dagger}$ is defined by the following formulas:

$$\begin{aligned} &\kappa_{E^\dagger}(f) = f(E^\dagger), \qquad (f \in \Lambda^0\mathcal{U}^\dagger), \\ &\kappa_{E^\dagger}(\{\varpi^\lambda\}_q) = (\langle \varpi^\lambda, \mathcal{E}_x\mathcal{V}\rangle \bmod \langle \Sigma^{[1]} + \Omega, \mathcal{E}_x\mathcal{V}\rangle), \\ &\kappa_{E^\dagger}(X_i^q(\omega^1, \cdots, \omega^p; \mathcal{U}^\dagger)) = L_i(\mathcal{E}^\dagger{}_x\mathcal{V}). \end{aligned} \tag{56}$$

Clearly, if $\mathcal{U}^\dagger \supseteq \mathcal{U}^{\dagger\prime}$, then $\kappa_{E^\dagger}(A'_q(\Sigma, \mathcal{U}^{\dagger\prime})) \supseteq \kappa_{E^\dagger}(A'_q, \mathcal{U}^\dagger))$. Set

$$\begin{aligned} A(E^\dagger) = \bigcup \{\kappa_{E^\dagger}(A'_q(\Sigma, \mathcal{U}^\dagger))\,;\ &\mathcal{U}^\dagger \text{ connected open} \\ &\text{neighborhood of } E^\dagger \text{ in } \mathfrak{G}^\dagger(\mathcal{V}, q)\}. \end{aligned} \tag{57}$$

$A(E^\dagger)$ is an ideal in $P(x)$. Set $X_i = [X^q{}_i(\omega^1, \cdots, \omega^p)](E^\dagger)$, (cf. (50)). Set $Y^\lambda = \langle \varpi^\lambda, \mathcal{E}_x\mathcal{V}\rangle$ modulo $\langle \Sigma^{[1]} + \Omega, \mathcal{E}_x\mathcal{V}\rangle$. These are elements in $P(x)$. Set

$$\xi_{\phi\,;ij}(E^\dagger) = \sum_{h=1}^{p-q} (A_{\phi\,;i\lambda}(x) \cdot Y^\lambda \cdot X_j - \mathrm{A}_{\phi\,;i\lambda}(x) \cdot Y^\lambda \cdot X_i) \tag{58}$$

Then we have

Proposition III. 6. $A(E^\dagger)$ is generated by all $\xi_{\phi;ij}(E^\dagger)$, $(\phi \in \Sigma^{[2]})$, and by all $Y^\lambda \cdot X$, $(X \in E^\dagger \subset \mathcal{E}^\dagger{}_x\mathcal{V})$. Assume further that $E^\dagger$ is in

$$\mathcal{U}^\dagger = \mathcal{U}^\dagger(\omega^1, \cdots, \omega^q),$$

(cf. $(5)^\dagger$). Then $A(E^\dagger) = \kappa_{E^\dagger}(A'_q(\Sigma, \mathcal{U}^\dagger))$ and $A(E^\dagger)$ is generated by all $\xi_{\phi;ij}(E^\dagger)$ $(\phi \in \Sigma^{[2]})$, and by all

$$(58)' \qquad \zeta_r{}^\lambda(E^\dagger) = Y^\lambda X_r + \sum_{h=1}^{p-q} {}^q w_r{}^h(E^\dagger) X_{q+h},$$
$$(\lambda = 1, \cdots, m; r = 1, \cdots, q).$$

Similarly, we shall set

$$(59) \qquad B(E^\dagger) = \bigcup \{\kappa_{E^\dagger}(E'_q(\Sigma, \mathcal{U}^\dagger)), \mathcal{U}^\dagger \text{ connected open neighborhood of } E^\dagger \text{ in } \mathfrak{G}^\dagger(\mathcal{V}, q)\}.$$

Then, by the definition of $B'_q(\Sigma, \mathcal{U}^\dagger)$,

$$(59)' \qquad B(E^\dagger) = Y(x) \cdot A(E^\dagger).$$

3. Hilbert's characteristic functions. Let $X_1, \cdots, X_p$ be p indeterminates. Order monomials $X_1{}^{k_1} \cdots X_p{}^{k_p}$ lexicographically. Let M be the set of all monomials of total degree l smaller than a fixed monomial of total degree l. Let k be the number of elements in M. Denote by $Q_l(k, p)$ the number of elements in the set $MX_1 \cup \cdots \cup MX_p$. It is easy to see that if l is sufficiently large compared with k, $Q_l(k, p)$ depends only on k and p. Thus we can define the integer $Q(k, p) = Q_l(k, p)$ for sufficiently large l. The function $Q(k, p)$ may be called the Macauly's function.

Let K be an arbitrary field and let I be an homogeneous ideal in the polynomial ring $K[X_1, \cdots, X_p]$, "homogeneous" means that $I = \sum_{l=0}^{\infty} I^{[l]}$, $I^{[l]} = I \cap K^{[l]}[X_1, \cdots, X_p]$, where $K^{[l]}[X_1, \cdots, X_p]$ is the submodule of all homogeneous polynomials of degree l. Set $\phi^l(I) =$ the dimension of the vector space $I^{[l]}$.

THEOREM III. 1. (Hilbert-Macauly). *For any homogeneous ideal I in $K[X_1, \cdots, X_p]$, there is an integer $l_0(I)$ satisfying the following conditions*:

$$\text{(i)} \qquad \phi^{l+1}(I) > Q(\phi^l(I), p), \quad \text{for } l < l_0(I),$$

$$\text{(ii)} \qquad \phi^{l+1}(I) = Q(\phi^l(I), p), \quad \text{for } l \geqq l_0(I).$$

For the proof, consult S. Bochner [1, p. 8].

When the ring $K[X_1, \cdots, X_p]$ has a double degree, i. e., $K[X_1, \cdots, X_p]$

$=\sum_{a,l} K^{[a,l]}[X_1,\cdots,X_p]$, and if an ideal I is homogeneous with respect to the double degree, we shall set $\phi^{a,l}(I)=$ the dimension of the vector space $I^{[a,l]}$.

The ring $\mathfrak{P}_q(\Sigma,\mathfrak{U}^\dagger)$ introduced in § 2 is a polynomial ring over the field $[\Lambda^0]\mathfrak{U}^\dagger$. Let $\mathfrak{P}_q^{[l]}(\Sigma,\mathfrak{U}^\dagger)$ be the module of all homogeneous polynomials of degree l. It has also a double degree, that is, the degree with respect to $[\mathbf{Y}^q](\Sigma,\mathfrak{U}^\dagger)$ and to $[\mathbf{X}^q](\Sigma,\mathfrak{U}^\dagger)$. Denote by $\mathfrak{P}_q^{[a,l]}(\Sigma,\mathfrak{U}^\dagger)$ the submodule of all homogeneous polynomials of degrees a and l with respect to $[\mathbf{Y}^q](\Sigma,\mathfrak{U}^\dagger)$ and to $[\mathbf{X}^q](\Sigma,\mathfrak{U}^\dagger)$, respectively. Similarly we define $P^{[l]}(x)$, $P^{[a,l]}(x)$. $P^{[a,l]}(x)$ is the submodule of all polynomials of degrees a and l with respect to $Y(x)$ and $\mathcal{E}^\dagger_x\mathfrak{V}$, respectively.

Definition III. 3.

$$\phi^l_q(\Sigma,\Omega)=\mathrm{Max}\{\phi^l(A_q(\Sigma,\mathfrak{U}^\dagger))\,;\ \mathfrak{U}^\dagger \text{ connected open set in } \mathfrak{G}^\dagger(\mathfrak{V},q)\},$$
$$\psi^l_q(\Sigma,\Omega)=\mathrm{Max}\{\phi^l(B_q(\Sigma,\mathfrak{U}^\dagger))\,;\ \mathfrak{U}^\dagger \text{ connected open set in } \mathfrak{G}^\dagger(\mathfrak{V},q)\},$$
$$t^l_q(\Sigma,\Omega)=\phi^{l+1}_q(\Sigma,\Omega)-\psi^{l+1}_q(\Sigma,\Omega).$$
$$\phi^l(\Sigma,E^\dagger)=\phi^l(A(E^\dagger)),\qquad \psi(\Sigma,E^\dagger)=\phi^l(B(E^\dagger)),$$
$$t^l(\Sigma,E^\dagger)=\phi^{l+1}(\Sigma,E^\dagger)-\psi^{l+1}(\Sigma,E^\dagger).$$

Since the dimension of the vector space $\mathfrak{P}_q^{[l]}(\Sigma,\mathfrak{U}^\dagger)$ is independent of $\mathfrak{U}^\dagger$, $\phi^l(\Sigma,\Omega)$ and $\psi^l(\Sigma,\Omega)$ are well defined integers. One sees easily by (59)′ that

$$t^l(\Sigma,E^\dagger)=\phi^{[1,l]}(A(E^\dagger)) \tag{60}$$

Let $\omega^1,\cdots,\omega^p$ be a base of Ω. Let E be an element in $\mathfrak{V}_l^q$ (cf. (36)). Let x be the origin of E. Then the set of all $(d\rho^l L \bmod \mathcal{E}^*_x\mathfrak{V})$, $L\in E$, forms a q-dimensional reduced contact element $E^\dagger=\mu(E)$ contained in $\mathfrak{U}^\dagger=\mathfrak{U}^\dagger(\omega^1,\cdots,\omega^q)$, where ρ^l is the projection of $\mathfrak{V}_l^q$ onto $\mathfrak{V}$. The mapping

$$\mu:\ \mathfrak{V}_l^q\rightarrow\mathfrak{U}^\dagger(\omega^1,\cdots,\omega^q) \tag{61}$$

is analytic and onto. By (39) and (46), it follows that

$$w_r^{q,h}(E)={}^q w_r^h(\mu(E)),\qquad (E\in\mathfrak{V}_l^q). \tag{60$'$}$$

Now we claim the following equality

$$t'(E)=t^l(\Sigma,\mu(E)),\qquad (E\in\mathfrak{V}_l^q). \tag{62}$$

(cf. (45)). To prove (62), denote by S the subspace of the conjugate space of $\mathcal{E}_x\mathfrak{R}_l$ generated by all $\langle du^\lambda_{i_1\cdots i_l},\mathcal{E}_x\mathfrak{R}\rangle=X^\lambda_{i_1\cdots i_l}$. Then $X^\lambda_{i_1\cdots i_l}=X^\lambda_{j_1\cdots j_l}$ for any permutation $j_1,\cdots,j_l$ of $i_1,\cdots,i_l$, and as far as the linear relations among $X^{\lambda}{}_{i_1\cdots i_l}$ are concerned, we can think of $X^{\lambda}{}_{i_1\cdots i_l}$ as indeterminates under the conditions of symmetry stated above. Let M be the subspace of S generated by

$$\bar{\xi}^{\lambda}{}_{\phi;ij;k_1\cdots k_{l-1}} = \sum_{\lambda=1}^{m} (A_{\phi;i\lambda}(y) X^{\lambda}{}_{jk_1\cdots k_{l-1}} - A_{\phi;j\lambda}(y) X^{\lambda}{}_{ik_1\cdots k_{l-1}})$$

$$\bar{\zeta}^{\lambda}{}_{k_1\cdots k_{l-1};r} = X^{\lambda}{}_{k_1\cdots k_{l-1}r} + \sum_{h=1}^{p-q} w_r{}^{q,h}(E) X^{\lambda}{}_{k_1\cdots k_{l-1}q+h}$$

$(\phi \in \Sigma^{[2]};\ \lambda = 1, \cdots, m;\ i, j, k_1, \cdots, k_{l-1} = 1, \cdots, p;\ r = 1, \cdots, q)$, where $y = \rho^l(x)$. Then by (45)

$$t'(E) = \dim M. \tag{62)'$$

Set $E^{\dagger} = \mu(E)$. Then

$$t(\Sigma, E^{\dagger}) = \dim (A(E^{\dagger})^{[1,l]}). \tag{62)''$$

By Proposition III. 6, $A(E^{\dagger})^{[1,l]}$ is a subspace of the vector space $(P(x))^{[1,l]}$ generated by all

$$\xi_{\phi;ij}(E^{\dagger}) \cdot X_{k_1} \cdots X_{k_{l-1}} = \sum_{\lambda=1}^{m} (A_{\phi;i\lambda}(y) Y^{\lambda} X_j X_{k_1} \cdots X_{k_{l-1}} \\ - A_{\phi;j\lambda}(y) Y^{\lambda} X_i X_{k_1} \cdots X_{k_{l-1}})$$

$$\zeta^{\lambda}{}_r(E^{\dagger}) \cdot X_{k_1} \cdots X_{k_{l-1}} = Y^{\lambda} X_{k_1} \cdots X_{k_{l-1}} X_r \\ + \sum_{h=1}^{p-q} {}^q w_r{}^h(E^{\dagger}) Y^{\lambda} X_{k_1} \cdots X_{k_{l-1}} X_{q+h}$$

$(\phi \in \Sigma^{[2]};\ \lambda = 1, \cdots, m;\ i, j, k_1, \cdots, k_{l-1} = 1, \cdots, p;\ r = 1, \cdots, q)$. Let a be the homomorphism of S onto the vector space $(P(x))^{[1,l]}$ defined by formulas: $a(Y^{\lambda} X_{k_1} \cdots, X_{k_l}) = X^{\lambda}{}_{k_1\cdots k_l}$. Then, by the remark in the beginning of this proof, a is an isomorphism. Comparing the system of generators of M and $(A(E^{\dagger})^{[1,l]})$, we see by (60)′ that a maps $A(E^{\dagger})$ upon M. Hence, by (62)′ and (62)″, the equality (62) holds.

LEMMA III. 1. *Let* $\mathfrak{W}$ *be a real analytic manifold. Take a system of indeterminates* $W_1, \cdots, W_a$. *Let* $F_1, \cdots, F_p$ *be linear elements in* $(\Lambda^0\mathfrak{W})[W_1, \cdots, W_a]$, *that is, linear combinations of* $W_1, \cdots, W_a$ *with coefficient analytic functions on* $\mathfrak{W}$. *Let* $\mathfrak{D}$ *be a connected open subset of* $\mathfrak{W}$. *Then* F_i *is considered as an element in* $(\Lambda^0\mathfrak{D})[W_1, \cdots, W_a]$, *by restriction. If there is* $\mathfrak{D}$ *such that* $F_1, \cdots, F_b$ *have a non-trivial linear relation in* $(\Lambda^0\mathfrak{D})[W_1, \cdots, W_a]$, *then* $F_1, \cdots, F_b$ *have also a non-trivial linear relation in* $(\Lambda^0\mathfrak{W})[W_1, \cdots, W_a]$.

Proof. By the restriction mapping, we can identify $K_1 = [\Lambda^0]\mathfrak{W}$ with a subfield of $K = [\Lambda^0]\mathfrak{D}$. This follows from the theorem of identity in the theory of functions of several complex variables. Set $F_i = \alpha^\mu{}_i W_\mu$, $\alpha^\mu{}_i \in K_1$. Assume that $\beta^i F_i = 0$, $\beta^i \in K$. Since K can be considered as a vector space over the field K_1, there is a base $\{e^\sigma\}$ such that any $\beta \in K$ can be expressed uniquely as $\beta = \beta_\sigma e^\sigma$, where $\beta_\sigma \in K_1$ and, for almost all σ, β_σ is zero. Set $\beta^i = \beta_\sigma{}^i e^\sigma$. Then $\beta^i F_i = 0$ implies that $\beta_\sigma{}^i F_i = 0$ for all σ. Then it follows easily that $F_1, \cdots, F_n$ have a non-trivial linear relation in $(\Lambda^0 \mathcal{W})[W_1, \cdots, W_n]$.

Proposition III. 7. Let $\omega^1, \cdots, \omega^q$ be linearly independent elements in Ω. Then, for any open connected set $\mathcal{U}^\dagger$ contained in $\mathcal{U}^\dagger(\omega^1, \cdots, \omega^q)$, $\phi^l(A_q(\Sigma, \mathcal{U}^\dagger)) = \phi^l(\Sigma, \Omega)$ and $\psi^l(B_q(\Sigma \mathcal{U}^\dagger)) = \psi^i(\Sigma, \Omega)$ and $t_q{}^l(\Sigma, \Omega$ $= \phi^{[1,l]}(A_q(\Sigma, \mathcal{U}^\dagger))$.

Proof. We shall show first that, for any connected open sets $\mathcal{U}^{\dagger\prime} \subset \mathcal{U}^\dagger$, $\phi^l(A_q(\Sigma, \mathcal{U}^\dagger)) = \phi^l(A_q(\Sigma, \mathcal{U}^{\dagger\prime}))$. By Proposition III. 5, there is a system of generators $F_1, \cdots, F_b$ of $A_q(\Sigma, \mathcal{U}^\dagger)$ such that the restrictions of $F_1, \cdots, F_b$ to $\mathcal{U}^{\dagger\prime}$ form a system of generators of $A_q(\Sigma, \mathcal{U}^{\dagger\prime})$. Then our contention follows from Lemma III. 1. In particular, we have

$$\phi^l(A_q(\Sigma, \mathcal{U}^\dagger)) = \phi^l(A_q(\Sigma, \mathcal{U}^\dagger(\omega^1, \cdots, \omega^q))).$$

Lemma III. 1 implies that, for any connected open subsets $\mathcal{W}^{\dagger\prime} \subseteq \mathcal{W}^\dagger$, $\phi^l(A_q(\Sigma, \mathcal{W}^{\dagger\prime})) \geqq \phi^l(A_q(\Sigma, \mathcal{W}^\dagger))$. Assume that $\phi^l{}_q(\Sigma, \Omega) = \phi^l(A_q(\Sigma, \mathcal{W}^\dagger))$. Since $\mathcal{U}^\dagger(\omega^1, \cdots, \omega^q)$ is everywhere dense in $\mathfrak{G}^\dagger(\mathcal{V}, q)$, there is a connected open set $\mathcal{U}^\dagger$ in $\mathcal{U}^\dagger(\omega^1, \cdots, \omega^q) \cap \mathcal{W}^\dagger$. Then $\phi^l(A_q(\Sigma, \mathcal{U}^\dagger)) = \phi^l{}_q(\Sigma, \Omega)$. Therefore for any $\mathcal{U}^{\dagger\prime}$ in $\mathcal{U}^\dagger(\omega^1, \cdots, \omega^q)$, $\phi^l{}_q(\Sigma, \Omega) = \phi^l(A_q(\Sigma, \mathcal{U}^{\dagger\prime}))$. The same argument proves the second equality. The third equality follows from the first two equalities and Definition III. 2.

By Proposition III. 7, the integer $l_0(A_q(\Sigma, \mathcal{U}^\dagger(\omega^1, \cdots, \omega^q)))$ (defined in Theorem III. 1) does not depend on the choice of $\omega^1, \cdots, \omega^q$. This integer will be denoted by $l_0(\Sigma, \Omega)$,

$$l_0(\Sigma, \Omega) = l_0(A_q(\Sigma, \mathcal{U}^\dagger(\omega^1, \cdots, \omega^q))). \tag{63}$$

LEMMA III. 2. *Let* $\omega^1, \cdots, \omega^p$ *be a base of* Ω. *Set* $\mathcal{U}^\dagger = \mathcal{U}^\dagger(\omega^1, \cdots, \omega^q)$. *Let* $F_1, \cdots, F_b$ *be elements in* $\mathcal{P}'_q(\Sigma, \mathcal{U}^\dagger)$. *Take* $E^\dagger$ *in* $\mathfrak{G}^\dagger$. *If* $\kappa_{E^\dagger}(F_1), \cdots,$ $\kappa_{E^\dagger}(F_b)$ *are linear independent, then* $F_1, \cdots, F_b$ *are also linearly independent in* $\mathcal{P}_q(\Sigma, \mathcal{U}^\dagger)$.

Proof. There is a neighborhood $\mathcal{N}^\dagger$ of $E^\dagger$ such that, for any $E^{\dagger\prime} \in \mathcal{N}^\dagger$, $\kappa_{E^{\dagger\prime}}(F_1), \cdots, \kappa_{E^{\dagger\prime}}(F_b)$ are also linearly independent. If $F_1, \cdots, F_b$ are not linearly independent, there is a non-trivial relation $\beta_1 F_1 + \cdots + \beta_b F_b = 0$, β_i is an analytic function on $\mathcal{U}^\dagger$. There is $E^{\dagger\prime}$ in $\mathcal{N}^\dagger$ such that $\beta_i(E^{\dagger\prime}) \neq 0$

for $i=1,\cdots,b$. Then $\kappa_{E^{\dagger}}(F_1),\cdots,\kappa_{E^{\dagger}}(F_b)$ are not linearly independent, which contradicts to the choice of $\mathfrak{N}^{\dagger}$.

Proposition III. 8. Let $E^{\dagger}$ be an element in $\mathfrak{G}^{\dagger}(\mathfrak{V}^{\dagger};q)$. Then,

(i) $$\phi^{l}(\Sigma,E^{\dagger})\leqq\phi^{l}_{q}(\Sigma,\Omega):$$

(ii) if $\phi^{l}(\Sigma,E^{\dagger})=\phi^{l}_{q}(\Sigma,\Omega)$, then $\psi^{l}(\Sigma,E^{\dagger})=\psi^{l}_{q}(\Sigma,\Omega)$;

(iii) if $E^{\dagger}\in\mathfrak{U}^{\dagger}=\mathfrak{V}^{\dagger}(\omega^1,\cdots,\omega^q)$ and if $F_1,\cdots,F_b$ are elements of degree l in $A'_q(\Sigma,\mathfrak{U}^{\dagger})$ such that $\kappa_{E^{\dagger}}(F_1),\cdots,\kappa_{E^{\dagger}}(F_b)$ form a base of $A^{[l]}(E^{\dagger})$, then $\phi^{l}(\Sigma,E^{\dagger})=\phi^{l}_{q}(\Sigma,\Omega)$ when and only when $F_1,\cdots,F_b$ a base of $A_q^{[l]}(\Sigma,\mathfrak{U}^{\dagger})$.

Proof. (i) and (iii) follow from Lemma III. 2. (ii) follows from Proposition III. 7.

4. **$\mathfrak{P}$-regular points.** Let (Σ,Ω) be a normal system on $\mathfrak{V}$. Let p be the number of independent variables. A point x of $\mathfrak{V}$ is called a $\mathfrak{P}$-semi-regular point of order l with respect to (Σ,Ω) if, for any $q=0,1,\cdots,p-1$, there is a q dimensional reduced contact element $E_q^{\dagger}$ to $\mathfrak{V}$ at x such that $\phi^{l+1}(\Sigma,E_q^{\dagger})=\phi^{l+1}_{q}(\Sigma,\Omega)$. A point x is called a $\mathfrak{P}$-regular point (with respect to (Σ,Ω)) if there is an integer l_0 such that x is a $\mathfrak{P}$-semi-regular point of order l for every $l\geqq l_0$. l_0 will be called a weight of the $\mathfrak{P}$ regular point x.

Set

(64) $S(\Sigma,\Omega,l)=\{$the set of all points which are not $\mathfrak{P}$-semi-regular points of order $l\}$;

(65) $S(\Sigma,\Omega)=\{$the set of all points which are not $\mathfrak{P}$-regular points$\}$.

Clearly we have

$$S(\Sigma,\Omega)=\bigcap_{l_0}\Big[\bigcup_{l\geqq l_0}S(\Sigma,\Omega,l)\Big]. \tag{66}$$

Definition III. 5. Let x be a point in $\mathfrak{V}$. Let $F^{\dagger}$ be a flag on $\mathcal{E}^{\dagger}_{x}\mathfrak{V}$ (Definition I. 11). Denote by $E_q^{\dagger}$ the q-th component of $F^{\dagger}$ $(q=0,1,\cdots,p-1)$. $F^{\dagger}$ is called a regular reduced flag (with respect to (Σ,Ω)), if there is an integer l_0 such that $\phi^{l+1}_{q}(\Sigma,\Omega)=\phi^{l+1}(\Sigma,E_q^{\dagger})$ for any $l\geqq l_0$ and any $q=0,1,\cdots,p-1$. l_0 will be called the weight of the regular reduced flag $F^{\dagger}$.

Denote by $\mathfrak{F}^{\dagger}(x)$ the set of all flags on $\mathcal{E}^{\dagger}_{x}\mathfrak{V}$. Set $\mathfrak{F}^{\dagger}\mathfrak{V}=\bigcup\{\mathfrak{F}(x);x\in\mathfrak{V}\}$. $\mathfrak{F}^{\dagger}\mathfrak{V}$ is an analytic manifold and $\mathfrak{F}^{\dagger}(x)$ is a submanifold of $\mathfrak{F}^{\dagger}\mathfrak{V}$. The main theorems of this section are the following:

THEOREM III. 2. *$S(\Sigma,\Omega)$ and $S(\Sigma,\Omega,l)$ are proper subvarieties of $\mathcal{V}$.*

THEOREM III. 3. *Let x be a $\mathcal{P}$-semi-regular point of order l' with respect to (Σ,Ω). If $l' \geqq l_0(\Sigma,\Omega)$, then x is a $\mathcal{P}$-regular point of weight l'* (cf. (63)).

THEOREM III. 4. *Let x be a $\mathcal{P}$-regular point of weight l_0. Assume that $l_0 \geqq l_0(\Sigma,\Omega)$. Then there is a regular reduced flag $F^\dagger$ on $\mathcal{E}^\dagger_x\mathcal{V}$ of weight l_0. Moreover, the set $\mathcal{R}\mathcal{F}^\dagger(\mathcal{V};l_0)$ of all reduced regular flags of weight l_0 is an open set in $\mathcal{F}^\dagger\mathcal{V}$.*

LEMMA III. 3. *Denote by $S(\Sigma,\Omega,l;q)$ the set of all $E^\dagger$ in $\mathcal{G}^\dagger(\mathcal{V},q)$ such that $\phi^{l+1}(\Sigma,E^\dagger) < \phi^{l+1}(\Sigma,\Omega)$. Then $S(\Sigma,\Omega,l;q)$ is a proper subvariety of $\mathcal{G}^\dagger(\mathcal{V},q)$.*

Proof. Take a base $\omega^1,\cdots,\omega^p$ of Ω. Set $\mathcal{U}^\dagger = \mathcal{U}(\omega^1,\cdots,\omega^p)$. It is sufficient to show that $S(\Sigma,\Omega,l;q) \cap \mathcal{U}^\dagger$ is a proper subvariety of $\mathcal{U}^\dagger$, since $\mathcal{U}^\dagger$ is an open subset of $\mathcal{G}^\dagger(\mathcal{V},q)$ and $\mathcal{G}^\dagger(\mathcal{V},q)$ is covered by such $\mathcal{U}^\dagger$'s. It is clear by Proposition III. 5 and (56) that, for any linearly independent $f_1,\cdots,f_b$ in $A'_q(\Sigma,\mathcal{U}^\dagger)$, the set of elements $E^\dagger$ in $\mathcal{U}^\dagger$ such that $\kappa_{E^\dagger}(f_1),\cdots,\kappa_{E^\dagger}(f_b)$ are linearly dependent forms a proper subvariety of $\mathcal{U}^\dagger$. It is also clear that there are homogeneous elements $f_1,\cdots,f_b$ in $A'_q(\Sigma,\mathcal{U}^\dagger)$ such that they $[\mathrm{A}^0]\mathcal{U}^\dagger$-generate $A^{[l+1]}{}_q(\Sigma,\mathcal{U}^\dagger)$ and such that, for any $E^\dagger$ in $\mathcal{U}^\dagger$, $\kappa_{E^\dagger}(f_1),\cdots,\kappa_{E^\dagger}(f_b)$ generate $A^{l+1}{}_q(\Sigma,E^\dagger)$. Then Propositions III. 8 (i) and (iii) imply that $E^\dagger$ is in $S(\Sigma,\Omega,l;q) \cap \mathcal{U}^\dagger$ if and only if, for any subset $f_{i_1},\cdots,f_{i_a}$ which is a base of $A^{[l+1]}{}_q(\Sigma,\mathcal{U}^\dagger)$, $\kappa_{E^\dagger}(f_{i_1}),\cdots,\kappa_{E^\dagger}(f_{i_a})$ are linearly dependent. Therefore $S(\Sigma,\Omega,l;q) \cap \mathcal{U}^\dagger$ is a proper subvariety of $\mathcal{U}^\dagger$.

LEMMA III. 4. *Let $S^\dagger$ be an element of $\mathcal{G}^\dagger(\mathcal{V},q)$ such that, for an integer l, $\phi^l{}_q(\Sigma,\Omega) = \phi^l(\Sigma,E^\dagger)$. Assume that $l \geqq l_0(\Sigma,\Omega)$. Then $\phi^{l+1}{}_q(\Sigma,\Omega) = \phi^{l+1}(\Sigma,E^\dagger)$.*

Proof. Let $\omega^1,\cdots,\omega^p$ be a base of Ω such that $\langle\omega^1,E^\dagger\rangle,\cdots,\langle\omega^q,E^\dagger\rangle$ are linearly independent. Set $\mathcal{U}^\dagger = \mathcal{U}^\dagger(\omega^1,\cdots,\omega^q)$. Then

$$\begin{aligned}
\phi^{l+1}{}_q(\Sigma,\Omega) &= \phi^{l+1}(A_q(\Sigma,\mathcal{U}^\dagger)), && \text{(by Prop. III. 7)},\\
&= Q(\phi^l(A_q(\Sigma,\mathcal{U}^\dagger)),p+m), && \text{(by Theorem III. 1)},\\
&= Q(\phi^l(A(E^\dagger)),p+m), && \text{(by the assumption)},\\
&\leqq \phi^{l+1}(A(E^\dagger)), && \text{(by Theorem III. 1)},\\
&= \phi^{l+1}(\Sigma,E^\dagger), && \text{(by Def. III. 3)}.
\end{aligned}$$

Therefore, Proposition III. 8 (i) implies that $\phi^{l+1}{}_q(\Sigma,\Omega) = \phi^{l+1}(\Sigma,E^\dagger)$.

By Lemma III. 4 it follows that the sequence $S(\Sigma,\Omega,l)$ for $l \geqq l_0(\Sigma,\Omega)$ is decreasing. Hence

$$S(\Sigma,\Omega)=\bigcap_{l} S(\Sigma,\Omega,l). \tag{66$'$}$$

Proof of Theorem 2. Take $\omega^1,\cdots,\omega^p$ and $\varpi^1,\cdots,\varpi^m$ as in Proposition III. 5. Denote tentatively by ρ the projection $\mathfrak{S}^{\dagger}(\mathfrak{V},q)\rightarrow\mathfrak{V}$. Set $\mathfrak{U}^{\dagger}=\mathfrak{U}(\omega^1,\cdots,\omega^q)$. Define the function ${}^{q}w_r{}^{h}$ by the formula (46). Let $\mathfrak{N}_{\epsilon}{}^{\dagger}$ be the set of all $E^{\dagger}$ in $\mathfrak{U}^{\dagger}$ such that $|{}^{q}w_r{}^{h}(E^{\dagger})|<\epsilon$ for any $r=1,\cdots,q$ and $h=1,\cdots,p-q$. Now there does not exist $E^{\dagger}$ in $\rho^{-1}(x)$ such that $\phi^{l+1}{}_q(\Sigma,\Omega)=\phi^{l+1}(\Sigma,E^{\dagger})$ if and only if $\rho^{-1}(x)\subseteq S(\Sigma,\Omega,l;q)$. Since $\rho^{-1}(x)$ is a connected submanifold of $\mathfrak{S}^{\dagger}(\mathfrak{V},q)$ and $S(\Sigma,\Omega,l;q)$ is a subvariety of $\mathfrak{S}^{\dagger}(\mathfrak{V},q)$, either $\rho^{-1}(x)\cap S(\Sigma,\Omega,l,q)=\rho^{-1}(x)$ or $\rho^{-1}(x)\cap S(\Sigma,\Omega,l,q)$ does not contain any non empty open subset of $\rho^{-1}(x)$. Therefore it follows that there does not exist $E^{\dagger}$ in $\rho^{-1}(x)$ such that $\phi^{l+1}{}_q(\Sigma,\Omega)=\phi^{l+1}(\Sigma,E^{\dagger})$ if and only if $\rho^{-1}(x)\cap\mathfrak{N}_{\epsilon}{}^{\dagger}\subseteq S(\Sigma,\Omega,l;q)$, because $\rho^{-1}(x)\cap\mathfrak{N}_{\epsilon}{}^{\dagger}$ is a non empty open subset of $\rho^{-1}(x)$.

Fix a point x in $\mathfrak{V}$. Take an open neighborhood N of x and ϵ so small that $S(\Sigma,\Omega,l;q)\cap\rho^{-1}(N)\cap\mathfrak{N}_{\epsilon}{}^{\dagger}$ is equal to the set of common zeros of functions $f_{\mu}(x,w)$ on $\rho^{-1}(N)\cap\mathfrak{N}_{\epsilon}{}^{\dagger}$. For any system of values $a\equiv(a_r{}^{h})$, $(|a_r{}^{h}|<\epsilon)$, denote by $f_{\mu}{}^{a}(x)=f_{\mu}(x,\cdots a_r{}^{h}\cdots)$. Denote by $S^{l}{}_q$ the set of all x' in $\mathfrak{V}$ such that there does not exist $E^{\dagger}$ in $\rho^{-1}(x)$ such that $\phi^{l+1}{}_q(\Sigma,\Omega)=\phi^{l+1}(\Sigma,E^{\dagger})$. Then the conclusion reached above implies that $S^{l}{}_q\cap N$ is equal to the common zeros of all $f_{\mu}{}^{a}$, that is, $S^{l}{}_q$ is a proper subvariety. Therefore $S(\Sigma,\Omega,l)=\bigcup\{S^{l}{}_q;q=0,1,\cdots,q-1\}$ is a proper subvariety. By (66)$'$, $S(\Sigma,\Omega)$ is also a subvariety.

Theorem III. 3 follows easily from Lemma III. 4. Theorem III. 4 follows easily from Theorem III. 2 and Lemma III. 4.

5. Regular bases. Let $L^{\dagger}$ be a reduced tangent vector to $\mathfrak{V}$ at x. We remark that $P^{[0,1]}(x)=\mathcal{E}^{\dagger}{}_x\mathfrak{V}\ni L^{\dagger}$ (cf. (55)) and so the product $v\cdot L^{\dagger}$ is defined for any $v\in P(x)$. Let $E^{\dagger}$, x as its origin, be an element in $\mathfrak{S}^{\dagger}(\mathfrak{V},q)$.

Definition III. 6. $L^{\dagger}$ is called l_1-prime to $E^{\dagger}$ (with respect to (Σ,Ω)) if the conditions $v\in P^{[1,l]}(x)$, $l\geqq l_1$, and $v\cdot L^{\dagger}\in A(E^{\dagger})$ always imply that v is in $A(E^{\dagger})$.

LEMMA III. 5. *Let $E^{\dagger}$ be an element in $\mathfrak{S}^{\dagger}(\mathfrak{V},q)$ $(q=0,1,\cdots,p-1)$. Then there is an integer $l_1=l_1(E^{\dagger})$ such that the set of reduced tangent* *vectors* $L^\dagger$ *at the origin* x *of* $E^\dagger$ *which are* l_1*-prime to* $E^\dagger$ *is everywhere dense in* $\mathcal{E}^\dagger{}_x\mathfrak{V}$.

Proof. Since $P(x)$ is a Noetherian ring, $A(E^\dagger)=\mathfrak{Q}_1\cap\cdots\cap\mathfrak{Q}_a$, where $\mathfrak{Q}_1,\cdots,\mathfrak{Q}_a$ are primary ideals of $P(x)$. It is well known that $\mathfrak{P}_\nu=\{v\in P(x)$; there is an integer τ such that $v^\tau\in\mathfrak{Q}_\nu\}$ is a prime ideal of $P(x)$. There is an integer μ_ν such that $\mathfrak{P}_\nu{}^{\mu_\nu}\subseteq\mathfrak{Q}_\nu$ $(\nu=1,\cdots,a)$. We can assume that, for $\nu=1,\cdots,b$ $(b\leqq a)$, and for any integer l, $\mathfrak{Q}_\nu$ does not contain $P^{[1,l]}(x)$, but that, for each $\nu=b+1,\cdots,a$, there is an integer $l(\nu)$ such that $\mathfrak{Q}_\nu\supseteq P^{[1,l]}(x)$ for any $l>l(\nu)$. b may be equal to zero. In this case $A^{[1,l]}(E^\dagger)=P^{[1,l]}(x)$ for $l\geqq l_1=\operatorname{Max}\{l(\nu)\,;\nu=1,\cdots,a\}$. Therefore any vector $L^\dagger$ in $\mathcal{E}^\dagger{}_x\mathfrak{V}$ is l_1-prime to $E^\dagger$. Hence we shall suppose that $b>0$. Put $l_1=\operatorname{Max}\{l(\nu)\,;\nu=b+1,\cdots,a\}$ if $b<a$, and $l_1=1$ if $b=a$. Set $A=\mathfrak{Q}_1\cap\cdots\mathfrak{Q}_b$. Then

$$A\cap P^{[1,l]}(x)=A^{[1,l]}(E^\dagger)\quad\text{for } l\geqq l_1. \tag{67}$$

The choice of b and the property $\mathfrak{P}_\nu{}^{\mu_\nu}\subseteq\mathfrak{Q}_\nu$ imply that $\mathfrak{P}_\nu\cap P^{[0,1]}(x)$ is a proper subspace of $\mathcal{E}^\dagger{}_x\mathfrak{V}=P^{[0,1]}(x)$ for $\nu=1,\cdots,b$. Assume that $L^\dagger\notin(\mathfrak{P}_1\cup\cdots\cup\mathfrak{P}_b)\cap P^{[0,1]}(x)$. Let v be an element of $P^{[1,l]}(x)$, where $l\geqq l_1$, such that $v\cdot L^\dagger\in A(E^\dagger)$. Then, for $\nu=1,\cdots,b$, $v\cdot L^\dagger\in\mathfrak{Q}_\nu$ and $L^\dagger\notin\mathfrak{P}_\nu$. Hence $v\in\mathfrak{Q}_\nu$, i.e., $v\in A=\mathfrak{Q}_1\cap\cdots\mathfrak{Q}_b$. Then (67) implies that $v\in A(E^\dagger)$. Thus the complementary set of $(\mathfrak{P}_1\cup\cdots\cup\mathfrak{P}_b)\cap\mathcal{E}^\dagger{}_x\mathfrak{V}$, which is everywhere dense, consists of vectors l_1-prime to $E^\dagger$.

Definition III. 7. Let $\omega^1,\cdots,\omega^p$ be an ordered base of Ω. Let x be a point in $\mathfrak{V}$. By a dual reduced flag at x to the ordered base $\omega^1,\cdots,\omega^p$ we mean the flag $F^\dagger$ on $\mathcal{E}^\dagger{}_x\mathfrak{V}$ such that the q-th component $E_q{}^\dagger$ of $F^\dagger$ satisfies the conditions: $\langle\omega^{q+1},E_q{}^\dagger\rangle=\cdots=\langle\omega^p,E_q{}^\dagger\rangle=0$ for $q=0,1,\cdots,p-1$ (cf. Definition III. 5).

Thus for each ordered base $\omega^1,\cdots,\omega^p$ of Ω, there is one and only one dual reduced flag at x to $\omega^1,\cdots,\omega^p$. Conversely, any reduced flag is the dual reduced flag of an ordered base, since for any base of Ω, the linear transformation of it by non-singular matrix with constant coefficients is again a base of Ω (note that $d\omega^i=0$).

Definition III. 8. An ordered base $\omega^1,\cdots,\omega^p$ of Ω is called l_1-regular at x (with respect to (Σ,Ω)), if it satisfies the following conditions:

(i) the dual reduced flag ${}^0F^\dagger$ at x to $\omega^1,\cdots,\omega^p$ is a regular reduced flag at x of weight l_1;

(ii) $X_i=L_i(\mathcal{E}^\dagger_x\mathfrak{V})$ (cf. $(6)^\dagger$ for $q=p$, $i=1,\cdots,p$), is l_1-prime to ${}^0E_{i-1}{}^\dagger$ for $i=1,\cdots,p$, where ${}^0E_i{}^\dagger$ is the i-th component of the reduced flag ${}^0F^\dagger$.

THEOREM III. 5. *Let (Σ,Ω) be a normal system. Let x be a $\mathfrak{P}$-regular point of weight l_0. Then there is an ordered base $\omega^1,\cdots,\omega^p$ of Ω which is l_1-regular at x for sufficiently large l_1.*

Proof. If x is a $\mathfrak{P}$-regular point of weight l_0, then x is a $\mathfrak{P}$-regular point of weight l for any $l\geqq l_0$. Therefore we can assume that $l_0\geqq l_0(\Sigma,\Omega)$. Take a regular flag $F^\dagger$ of weight l_0 at x (Theorem III. 4). Let $E_q{}^\dagger$ be the q-th component of $F^\dagger$. Then there is a neighborhood $\mathfrak{N}_q$ of $E_q{}^\dagger$ in the manifold of all q dimensional subspaces of $\mathcal{E}^\dagger_x\mathfrak{V}$ such that any reduced flag ${}'F^\dagger$, of which q-th component is in $\mathfrak{N}_q$ for $q=1,\cdots,p-1$, is again a reduced regular flag at x of weight l_0 (cf. Theorem III. 4). Let us choose $\mathfrak{N}_q$ in such a way that, for any ${}'E_q{}^\dagger$ in $\mathfrak{N}_q$, the set of all vectors $L^\dagger$ in $\mathcal{E}^\dagger_x\mathfrak{V}$ such that the space spanned by ${}'E_q{}^\dagger$ and $L^\dagger$ is in $\mathfrak{N}_{q+1}$ contains an interior point for $q=0,\cdots,p-2$. Set ${}^0E_0{}^\dagger=\{x\}$. Then, by Lemma III. 5, there is a vector $L_1{}^\dagger$ in $\mathcal{E}^\dagger_x\mathfrak{V}$ which is l^0-prime to ${}^0E_0{}^\dagger$ and the space ${}^0E_1{}^\dagger$ spanned by $L_1{}^\dagger$ and ${}^0E_0{}^\dagger$ is in $\mathfrak{N}_1$, where $l^0=l_1({}^0E_0{}^\dagger)$ (cf. Lemma III. 5). Continuing this process, we can choose easily ${}^0E_q{}^\dagger$ in $\mathfrak{N}_q$ and $L_{q+1}{}^\dagger$ in $\mathcal{E}^\dagger_x\mathfrak{V}$ $(q=0,1,\cdots,p-1)$ such that $\{{}^0E_q{}^\dagger\}$ form a reduced flag at x, ${}^0E_{q+1}{}^\dagger$ is generated by ${}^0E_q{}^\dagger$ and by $L_{q+1}{}^\dagger$, and such that $L_{q+1}{}^\dagger$ is l^q-prime to ${}^0E_q{}^\dagger$, where $l^q=l_1({}^0E_q{}^\dagger)$. Set $l_1=\mathrm{Max}\{l^0,\cdots,l^{q-1}\}$. Then it is easy to see that an ordered base of Ω such that ${}^0F^\dagger$ is the dual reduced flag to the base is l_1-regular at x, since if X is l-prime to ${}^0E_q{}^\dagger$ then any vector in the space spanned by X and ${}^0E_q{}^\dagger$ but not in ${}^0E_q{}^\dagger$ is again l-prime to ${}^0E_q{}^\dagger$.

THEOREM III. 6. *Let (Σ,Ω) be a normal system with p independent variables. Then there is an integer $l_1(\Sigma,\Omega)$ such that for $l\geqq l_1(\Sigma,\Omega)$*

$$t^l{}_q(\Sigma,\Omega)=n_{l-1}-t^{l-1}{}_{q-1}(\Sigma,\Omega)+t^l{}_{q-1}(\Sigma,\Omega)$$

where $1\leqq q\leqq p$ and $n_l=mC_l^{p+l-1}$.

Proof. By Theorem III. 2 there is a $\mathfrak{P}$-regular point x of weight l_0. By Theorem III. 5, there is an ordered base $\omega^1,\cdots,\omega^p$ of Ω which is l_1-regular at x. Let $F^\dagger$ be the dual reduced flag at x to $\omega^1,\cdots,\omega^p$. Let $E_q{}^\dagger$ $(q=0,1,\cdots,p)$ be the q-th component of $F^\dagger$. Then $\phi^l{}_q(\Sigma,\Omega)=\phi^l(\Sigma,E_q{}^\dagger)$ for $l\geqq l_1$. Hence by Definition III. 3, Proposition III. 8 (ii),

$$t^l{}_q(\Sigma,\Omega)=t^l(\Sigma,E_q{}^\dagger)\qquad(l\geqq l_1-1). \tag{68}$$

Let $X_1, \cdots, X_p$ be the base in $\mathcal{E}^{\dagger}{}_x\mathcal{V}$ dual to $\langle\omega^1, \mathcal{E}^{\dagger}{}_x\mathcal{V}\rangle, \cdots, \langle\omega^p, \mathcal{E}^{\dagger}{}_x\mathcal{V}\rangle$. Then $E_q{}^{\dagger}$ is generated by $X_1, \cdots, X_q$. By Proposition III. 6, $A(E_q{}^{\dagger})^{[1,l]}$ is generated as a vector space by all

$$\xi_{\phi\,;ij}(E_q{}^{\dagger}) \cdot X_{k_1} \cdots X_{k_{l-1}} \text{ and } \zeta^{\lambda}{}_r(E_q{}^{\dagger}) \cdot X_{k_1} \cdots X_{k_{l-1}}$$

$$(\phi \in \Sigma^{[2]}\,; i, j, k_1, \cdots, k_{l-1} = 1, \cdots, p\,; \lambda = 1, \cdots, m\,; r = 1, \cdots, q),$$

for each q. Therefore since $\xi_{\phi\,;ij}(E_q)^{\dagger} = \xi_{\phi\,;ij}(E_{q-1}{}^{\dagger})$ and $\xi^{\lambda}{}_{r'}(E_q{}^{\dagger}) = \xi^{\lambda}{}_{r'}(E_{q-1}{}^{\dagger})$ for $r' = 1, \cdots, q-1$,

$$A(E_q{}^{\dagger})^{[1,l]} = A(E_{q-1}{}^{\dagger})^{[1,l]} + \sum_{\lambda=1}^{m} \xi^{\lambda}{}_q(E_q{}^{\dagger}) P^{[0,l-1]}(x)$$

for $q \geqq 1$. On the other hand ${}^q w_q{}^h(E_q{}^{\dagger}) = 0$ for $h = 1, \cdots, p-q$, since $F^{\dagger}$ is the dual reduced flag at x to $\omega^1, \cdots, \omega^p$. Hence, by (58)$'$, $\xi^{\lambda}{}_q(E_q{}^{\dagger}) = Y^{\lambda}X_q$. Then, for $q \geqq 1$,

$$A(E_q{}^{\dagger})^{[1,l]} = A(E_{q-1}{}^{\dagger})^{[1,l]} + X_q P^{[1,l-1]}(x),$$

since $P^{[1,l-1]}(x) = Y^1 P^{[0,l-1]}(x) + \cdots + Y^m P^{[0,l-1]}(x)$. Let $v_1, \cdots, v_a$ be a base of $P^{[1,l-1]}(x)$ modulo $A(E_{q-1}{}^{\dagger})^{[1,l-1]}$. Then

$$A(E_q{}^{\dagger})^{[1,l]} = A(E_{q-1}{}^{\dagger})^{[1,l]} + X_q \cdot \boldsymbol{R}v_1 + \cdots + X_q \cdot \boldsymbol{R}v_a.$$

Since $\omega^1, \cdots, \omega^p$ is l_1-regular, X_q is l_1-prime to $A(E_{q-1}{}^{\dagger})$. Therefore it follows that the above sum is a direct sum, that is,

$$t^l(\Sigma, E_q) = \dim(A(E_q{}^{\dagger})^{[1,l]}) = t^l(\Sigma, E_{q-1}{}^{\dagger}) + a.$$

By the definition of a, $a = n_{l-1} - t^{l-1}(\Sigma, E_{q-1})$. Hence

$$(69) \qquad t^l(\Sigma, E_q{}^{\dagger}) = n_{l-1} - t^{l-1}(\Sigma, E_{q-1}{}^{\dagger}) + t^l(\Sigma, E_{q-1}{}^{\dagger}) \qquad (l \geqq l_1)$$

Then the theorem follows from (68) and (69).

6. The fundamental theorem. Let (Σ', Ω') be an exterior differential system with independent variables on a real analytic manifold $\mathcal{V}'$.

Definition III. 9. An integral point y of (Σ', Ω') is called normal if y is an ordinary integral point and if there is a neighborhood $\mathcal{N}$ of y in $\mathcal{V}'$ such that for any y' in $\mathcal{N} \cap \mathfrak{J}^0\Sigma'$

$$(70) \qquad \langle \Sigma'^{[1]} \cap \Omega', \mathcal{E}_{y'}\mathcal{V}' \rangle = 0.$$

Proposition III. 9. If (Σ', Ω') is involutive at an integral point y, then y is normal.

Proof. By Definition I.17, y must be an ordinary integral point and there is a p dimensional integral element E of (Σ', Ω') at y such that $\langle \Omega', E \rangle$ is p dimensional, where p is the number of independent variables in Ω'. Let $\omega^1, \cdots, \omega^p$ be a base of Ω'. By Proposition I.6, there is a neighborhood $\mathcal{N}$ of y in $\mathcal{V}'$ such that, for any y' in $\mathcal{N} \cap \mathcal{J}^0\Sigma'$, there is an an integral element E' on which $\omega^1, \cdots, \omega^p$ are linearly independent. Take an element $a_1\langle \omega^1, \mathcal{E}_{y'}\mathcal{V}' \rangle + \cdots + a_p\langle \omega^p, \mathcal{E}_{y'}\mathcal{V}' \rangle \in \langle \Sigma' \cap \Omega', \mathcal{E}_{y'}\mathcal{V}' \rangle$. Since $\langle \Sigma'^{[1]} \cap E' \rangle = 0$, $\langle a_1\omega^1 + \cdots + a_p\omega^p, E' \rangle = 0$, that is $a_1 = \cdots = a_p = 0$. Therefore y is a normal point.

THEOREM III.7. *Let (Σ, Ω) be a normal system on $\mathcal{V}$. Let x be a $\mathcal{P}$-regular point iwth respect to (Σ, Ω). Let $\omega^1, \cdots, \omega^p$ be an ordered base of Ω which is l_1-regular. Construct $(\mathcal{R}_l\Sigma, \Omega)$ by the base $\omega^1, \cdots, \omega^p$. Let y be an integral point of $(\mathcal{R}_l\Sigma, \Omega)$. Assume that $l \geqq l_1$ and that $\rho_0{}^l(y) = x$, where $\rho_0{}^l$ is the projection of $\mathcal{R}$ onto $\mathcal{V} = \mathcal{R}_0$. Then $(\mathcal{R}_l\Sigma, \Omega)$ is involutive at y if and only if y is a normal point of $(\mathcal{R}_l\Sigma, \Omega)$. Moreover if y is normal, and if E is p-dimensional integral element of $(\mathcal{R}_l\Sigma, \Omega)$ at y, then the system of characters of E is given by the following formula:*

$$s_0(E) = t^l{}_0(\Sigma, \Omega) + n - p + m\left(\sum_{\nu=1}^{l-1} C_\nu{}^{p+\nu-1}\right);$$

$$s_q(E) = t^l{}_q(\Sigma, \Omega) - t^l{}_{q-1}(\Sigma, \Omega) \text{ for } q = 1, \cdots, p-1,$$

where p is the number of independent variables in Ω.

Proof. By Proposition III.9, it is sufficient to show that, if y is normal, then $(\mathcal{R}_l\Sigma, \Omega)$ is involutive at y. Let $\mathcal{N}_l$ be a neighborhood of y such that, for any $y' \in \mathcal{N}_l \cap \mathcal{J}^0\mathcal{R}_l\Sigma$,

$$\langle \mathcal{R}_l\Sigma^{[1]} \cap \Omega, \mathcal{E}_{y'}\mathcal{R}_l \rangle = 0. \tag{71}$$

Let $F^\dagger$ be the dual reduced flag at x to $\omega^1, \cdots, \omega^p$. Denote by $E_q{}^\dagger$ the q-th component of $F^\dagger$. Then there is a neighborhood $\mathcal{N}_q{}^\dagger$ of $E_q{}^\dagger$ in $\mathcal{G}^\dagger(\mathcal{V}, q)$ such that, for any $E^\dagger$ in $\mathcal{N}_q{}^\dagger$, we have the equality

$$t^l{}_q(\Sigma, \Omega) = t^l(\Sigma, E^\dagger), \tag{72}$$

because $\omega^1, \cdots, \omega^p$ is a l_1-regular base (cf. Lemma III.3 and Lemma III.4. We can choose $\mathcal{N}_q{}^\dagger$ in such a way that $\rho_0{}^l(\mathcal{N}_l) \supseteqq \mathcal{N}_0{}^\dagger$ and such that $\eta^\dagger{}_q(\mathcal{N}^\dagger{}_q) \subseteqq \mathcal{N}^\dagger{}_{q-1}$ (cf. (47)). First we maintain the following, for $q = 0, 1, \cdots, p-1$.

$(*)_q$: Let E be a q-dimensional integral element of $(\mathcal{R}_l\Sigma, \Omega)$ such that $\mu(E)$ (cf. (61)), is in $\mathfrak{N}^\dagger_q$ and such that its origin is in $\mathfrak{N}_l$. Then

$$\begin{aligned}\dim J(E) &= \dim\, (J(E) \bmod \langle \Omega, \mathcal{E}_{y'}\mathcal{R}_l\rangle) \\ &= t^l{}_q(\Sigma, \Omega) + n - p + m(\sum_{\nu=1}^{l-1} C_\nu{}^{p+\nu-1}),\end{aligned}$$

where y' is the origin of E. By Proposition II. 4, (45), and (45)$'$,

$$\begin{aligned}\dim (J(E) \bmod \langle \Omega, \mathcal{E}_{y'}\mathcal{R}_l\rangle) &= t'(E) + n - p + m(\sum_{\nu=1}^{l-1} (C_\nu{}^{p+\nu-1})) \\ \leqq \dim\, (\langle A_l{}^q, \mathcal{E}_{y'}\mathcal{R}_l\rangle_E) &+ n - p + m(\sum_{\nu=1}^{l-1} (C_\nu{}^{p-\nu-1})) = \dim\, (J(E)).\end{aligned}$$

Therefore, by (62) and (72), it is sufficient to show that

$$(73)_q \qquad \dim \langle A_l{}^q, \mathcal{E}_{y'}\mathcal{R}_l\rangle_E = t^l{}_q(\Sigma, \Omega).$$

We shall prove this equality by induction on q. Let y' be an integral point in $\mathfrak{N}_0$. Then, since $\langle A_l{}^0, \mathcal{E}_{y'}\mathcal{R}_l\rangle \subseteq \langle \mathcal{R}_l\Sigma^{[1]}, \mathcal{E}_{y'}\mathcal{R}_l\rangle$, (71) implies that $\dim \langle A_l{}^0, \mathcal{E}_{y'}\mathcal{R}_l\rangle = \dim \langle A'_l{}^0, \mathcal{E}_{y'}\mathcal{R}_l\rangle = t^l{}_0(\Sigma, y') = t^l{}_0(\Sigma, \Omega)$. Assume that $(73)_{q-1}$ is proved and that E is a q-dimensional integral element of $\mathcal{R}_l\Sigma$ such that $\mu(E) \in \mathfrak{N}_q{}^\dagger$. Then $E' = \eta_q(E)$ is a $q-1$-dimensional integral element of $\mathcal{R}_l\Sigma$ such that $\mu(E') \in \mathfrak{N}_{q-1}{}^\dagger$. Hence by Proposition II. 6, (45), (62), (72), and $(73)_{q-1}$,

$$t^l{}_q(\Sigma, \Omega) \leqq \dim \langle A_l{}^q, \mathcal{E}_{y'}\mathcal{R}_l\rangle_E \leqq t^l{}_{q-1}(\Sigma, \Omega) + n_{l-1} - t^{l-1}{}_{q-1}(\Sigma, \Omega),$$

since $\mu(d\rho_{l-1}{}^l E') = \mu(E')$. Then Theorem III. 6 implies the equality $(73)_q$. Therefore we have proved $(*)_q$ for $q = 0, 1, \cdots, p-1$.

Now let E be a p dimensional integral element of $(\mathcal{R}_l\Sigma, \Omega)$. Then there is a unique subspace E_q of E such that $\mu(E_q) = E_q{}^\dagger$ for $q = 0, 1, \cdots, p$. The spaces E_q form a flag on E. Let $\mathfrak{N}_{l,q}$ be a neighborhood of E_q such that $\rho(\mathfrak{N}_{l,q}) \subseteq \mathfrak{N}_l$ and $\mu(\mathfrak{N}_{l,q}) \subseteq \mathfrak{N}_q{}^\dagger$. Then for any $E \in \mathfrak{N}_{l,q} \cap \mathfrak{J}^q\mathcal{R}_l\Sigma$,

$$\dim J(E) = t^l{}_q(\Sigma, \Omega) + n - p + m(\sum_{\nu=0}^{l-1} C_\nu{}^{p+\nu-1})$$

for $q = 0, 1, \cdots, p-1$. This shows that, on a neighborhood of E_q in $\mathfrak{J}^q\mathcal{R}_l\Sigma$, the rank of system of polar forms remains constant, for $q = 0, 1, \cdots, p-1$. Therefore E is an ordinary integral element. Moreover we have the formulas:

$$\begin{aligned}s_0(E) &= t^l{}_0(\Sigma, \Omega) + n - p + m(\sum_{\nu=1}^{l-1} C_\nu{}^{p+\nu-1}); \\ s_q(E) &= t^l{}_q(\Sigma, \Omega) - t^l{}_{q-1}(\Sigma, \Omega) \quad \text{for } p-1 \geqq q \geqq 1; \\ s_p(E) &= mC_l{}^{p+l-1} - t^l{}_{p-1}(\Sigma, \Omega).\end{aligned}$$

We must show that there is at least one q dimensional integral element E of origin y. By $(*)_0$, we know that $\dim J(y) = \dim(J(y) \bmod \langle \Omega, \mathcal{E}_y \mathfrak{R}_l \rangle)$. Therefore we can solve the equation $J(y) = 0$, under the conditions:

$$\langle \omega^1, \mathcal{E}_y \mathfrak{R}_l \rangle = 1, \langle \omega^2, \mathcal{E}_y \mathfrak{R}_l \rangle = \cdots = \langle \omega^p, \mathcal{E}_y \mathfrak{R}_l \rangle = 0.$$

Let L_1 be a solution. Let E_1 be the 1-dimensional contact element spanned by L_1. Then E_1 is 1-dimensional integral element of $\mathfrak{R}_l \Sigma$ such that $\mu(E_1) = E_1{}^{\dagger}$. Then, since $\dim J(E_1) = \dim(J(E_1) \text{ modulo } \langle \Omega, \mathcal{E}_y \mathfrak{R}_l \rangle)$ by $(*)_1$, there is a tangent vector L_2 to $\mathfrak{R}_l$ at y such that $\langle J(E_1), L_2 \rangle = 0$, $\langle \omega^2, L_2 \rangle = 1$, $\langle \omega^1, L_2 \rangle = \langle \omega^3, L_2 \rangle = \cdots = \langle \omega^p, L_2 \rangle = 0$. Then the contact element E_2 spanned by E_1 and L_2 is an integral element such that $\mu(E_2) = E_2{}^{\dagger}$. Repeating this process, we can obtain a p dimensional integral element E at y on which $\omega^1, \cdots, \omega^p$ are linearly independent. Therefore $(\mathfrak{R}_l \Sigma, \Omega)$ is involutive at y.

FUNDAMENTAL THEOREM. *Let* (Σ, Ω) *be a normal system with* p *independent variable on* $\mathfrak{V}$. *Let* $\mathfrak{P}^l(\Sigma, \Omega)$ *be the* l*-th prolongation of* (Σ, Ω). $\mathfrak{P}^l(\Sigma, \Omega)$ *is defined on* $\mathfrak{G}^l(\mathfrak{V}, p) = \mathfrak{V}_l$. *Let* ρ^l *be the natural projection of* $\mathfrak{V}_l$ *onto* $\mathfrak{V}$. *Let* x *be a* $\mathfrak{P}$*-regular point of* (Σ, Ω). *Then there is an integer* $l_1(x)$ *satisfying the following conditions: if* y *is an integral point of* $\mathfrak{P}^l(\Sigma, \Omega)$ *and if* $l \geqq l_1(x)$ *then* $\mathfrak{P}^l(\Sigma, \Omega)$ *is involutive at* y *if and only if* y *is a normal point of* $\mathfrak{P}^l(\Sigma, \Omega)$. *In this case the sytem of characters of a* p*-dimensional integral element* E *at* y *is given by the following formula*

$$s_0(E) = t^l{}_0(\Sigma, \Omega) + n - p + m\Big(\sum_{\nu=1}^{l-1} (C_\nu{}^{p+\nu-1})\Big) + c_l;$$

$$s_q(E) = t^l{}_q(\Sigma, \Omega) - t^l{}_{q-1}(\Sigma, \Omega) \text{ for } q = 0, 1, \cdots, p-1;$$

$$s_p(E) = mC_l{}^{p+l-1} - t^l{}_{p-1}(\Sigma, \Omega).$$

where $c_l = \sum_{\nu=0}^{l-1} (p+1)^{l-1-\nu} c'_l$, $c'_{\mathrm{c}} = \alpha_1 p$,

$$c'_\nu = \alpha\ p + mp\tfrac{1}{2}(p-1)(C_{\nu-1}{}^{p+\nu-2}) + \sum_{h=1}^{\nu-1} (C_h{}^{p+h-1})$$

for $\nu \geqq 1$, and α_1 is the maximal number of linearly independent Pfaffian forms in $\Sigma^{[1]}$.

Proof. By Theorem III. 5, there is an ordered base $\omega^1, \cdots, \omega^p$ of Ω which is l_1-regular at x. Set $l_1(x) = l_1$. Then the theorem follows easily from Theorem II. 2, Theorem III. 7, and from Proposition II. 1.

7. An example. If one replaces the condition (70) by the following weaker condition:

$$\langle d(\Sigma')^{[0]} \cap \Omega', \mathcal{E}_y{}'\mathfrak{V}' \rangle = 0 \tag{74}$$

then the Fundamental theorem does not hold for this definition of normal point, that is, (70) does not imply (74), as one can see easily by the following.

Example 2. Let $\mathfrak{V}$ be a 4-dimensional euclidean space with a system of coordinates (x_1, x_2, u^1, u^2). Set $\omega^1 = dx_1$, $\omega^2 = dx_2$, $\varpi^1 = du^1$, and $\varpi^2 = du^2$. Let Ω be the system of 2 independent variables generated by ω^1 and ω^2. Let Σ be the exterior differential system generated by

$$\phi_{(1)} = x_2 \omega^1 \wedge \varpi^1 + u^1 \omega^1 \wedge \omega^2;$$

$$\phi_{(2)} = -x_1 \omega^2 \wedge \varpi^2 + u^2 \omega^1 \wedge \omega^2;$$

$$\phi_{(3)} = \omega^1 \wedge \varpi^1 + \omega^2 \wedge \varpi^2.$$

Clearly the subspace: $u^1 = u^2 = 0$ is an integral manifold of (Σ, Ω). We shall show that (i) there exists a $\mathfrak{P}$-regular point P such that $u^1(P) = u^2(P) = 0$, $x^1(P) \neq 0$, $x^2(P) \neq 0$, (ii) if y is any integral point of $\mathfrak{P}^l(\Sigma, \Omega)$ such that $\rho^l(y) = P$, y is an ordinary integral point and satisfies (74) but not (70).

By Theorem II. 2, it is sufficient to observe $(\mathcal{R}_l\Sigma, \Omega)$. It is easy to see that

$$\Theta_{(1)12;} = x_2 u^1{}_2 + u^1; \quad \Theta_{(2)12;} = x_1 u^2{}_1 + u^2; \quad \Theta_{(3)12;} = u^1{}_2 - u^2{}_1, \cdots.$$

$$\Theta_{(1)12;k_1\cdots k_l} = x_2 u^1{}_{2\,k_1\cdots k_l} + (1 + \sum_{\nu=1}^{l} \delta_{k_\nu}{}^2) u^1{}_{k_1\cdots k_l};$$

$$\Theta_{(2)12;k_1\cdots k_l} = x_1 u^2{}_{1\,k_1\cdots k_l} + (1 + \sum_{\nu=1}^{l} \delta_{k_\nu}{}^1) u^2{}_{k_1\cdots k_l};$$

$$\Theta_{(3)12;k_1\cdots k_l} = u^1{}_{2\,k_1\cdots k_l} - u^2{}_{1\,k_1\cdots k_l}.$$

Thus the coefficients of elements in $(A'_l{}^q)$, when they are written by power series of x_1, x_2, u^1, u^2, do not contain u^1 and u^2. Hence if P' is a $\mathfrak{P}$-regular point, then the point P such that $x^1(P) = x^1(P')$, $x^2(P) = x^2(P')$, $u^1(P) = u^2(P) = 0$, is also a $\mathfrak{P}$-regular point. Moreover, it is clear that there is a $\mathfrak{P}$-regular point P' such that $x^1(P') \neq 0$ and $x^2(P') \neq 0$ (Theorem III. 2). This proves (i). Set

$$\epsilon(k_1, \cdots, k_l) = (-1)^{l+1} \prod_{\nu=1}^{l-1} (1 + \sum_{\mu=\nu+1}^{l} \delta_{k_\mu}{}^{k_\nu}), \quad (l \geqq 2).$$

Then it is easy to see that $\epsilon(k_1,\cdots,k_l)=\epsilon(k_{\pi(1)}\cdots k_{\pi(l)})$ for any permutation π of l letters, and that

$$\begin{aligned}\epsilon(1,2,k_1,\cdots,k_l) &= -\,(1+\sum_{\nu=1}^{l}\delta_{k_\nu}{}^{2})\cdot\epsilon(1,k_1,\cdots,k_l)\\ &= -\,(1+\sum_{\nu=1}^{l}\delta_{k_\nu}{}^{1})\cdot\epsilon(2,k_1,\cdots,k_l).\end{aligned}$$

Now $\mathcal{R}_l$ is a euclidean space of dimensions $4+2\sum_{\nu=1}^{l}(\nu+1)$, with the system of coordinates

$$(x_1,x_2,u^1,u^2,\cdots,u^{\lambda}{}_{k_1\cdots k_\nu},\cdots),\qquad(\nu=1,\cdots,l;k_1,\cdots,k_\nu,\lambda=1,2).$$

Denote by $\mathcal{R}'_l$ the open set of $\mathcal{R}_l$ formed by all points such that $x^1\neq0$ and $x^2\neq0$. It is easy to see that $'\mathfrak{J}^0\mathcal{R}_l\Sigma\cap\mathcal{R}_l'$ is the submanifold of $\mathcal{R}_l'$ defined by the conditions:

$$\begin{aligned}&u^1{}_{2\,k_1\cdots k_{l-1}}=\epsilon(1,2,k_1,\cdots,k_{l-1})\cdot u^1\cdot(x_2x_{k_1}\cdots k_{l-1})^{-1};\\ &u^2{}_{1\,k_1\cdots k_{l-1}}=\epsilon(1,2,k_1,\cdots,k_{l-1})\cdot u^2\cdot(x_1x_{k_1}\cdots k_{l-1})^{-1};\\ &x_1u^1=x_2u^2=u.\end{aligned}$$

Thus the dimension of the submanifold $'\mathfrak{J}^0\mathcal{R}_l\Sigma\cap\mathcal{R}_l'$ is 5 and the system of functions $x_1,x_2,u^1{}_{a_1\cdots a_l},u^2{}_{b_1\cdots b_l}$, where $a_1=\cdots=a_l=1$ and $b_1=\cdots=b_l=1$, and u can be considered as a system of coordinates on $'\mathfrak{J}^0\mathcal{R}_l\Sigma\cap\mathcal{R}_l'$. It is not hard to see that

$$\begin{aligned}&d\Theta_{(1)12;\,k_1\cdots k_\nu},\quad d\Theta_{(2)12;\,k_1\cdots k_\nu},\quad d\Theta_{(3)12;\,a_1\cdots a_{\nu'}},\quad\text{and}\quad d\Theta_{(3)12;\,b_1\cdots b_{\nu'}}\\ &\qquad(\nu,\nu'=0,1,\cdots,l-1;a_1=\cdots=a_{\nu'}=1;\\ &\qquad\qquad\qquad b_1=\cdots=b_{\nu'}=2;2\geqq k_1\geqq\cdots\geqq k_\nu),\end{aligned}$$

are linearly independent modulo Ω at each point of $\mathcal{R}_l'$. Their number is equal to $\dim\mathcal{R}_l-5$. Therefore any point in $'\mathfrak{J}^0\mathcal{R}_l\Sigma\cap\mathcal{R}_{l'}$ is an ordinary integral point and satisfies (74). If y is in $'\mathfrak{J}^0\mathcal{R}_l\Sigma\cap\mathcal{R}_l'$ and if $a_1=\cdots=a_l=1$,

$$\begin{aligned}&x_1d\Theta_{(1)12;\,a_1\cdots a_{l-1}}-x_2d\Theta_{(2)12;\,a_1\cdots a_{l-1}}-x_1x_2d\Theta_{(3)12;\,a_1\cdots a_{l-1}}\\ &\qquad\equiv(x_1u^1{}_{a_1\cdots a_l}(y)+(l+1)!\,u(y)\cdot(x_1)^{-l})\,\omega^1\end{aligned}$$

at y modulo ω^2 and Π_l. Since $u^1{}_{a_1\cdots a_l},x_1$, and u are independent variables on $'\mathfrak{J}^0\mathcal{R}_l\Sigma\cap\mathcal{R}_l'$, it follows that y is not a normal point of $(\mathcal{R}_l\Sigma,\Omega)$.

INSTITUTE FOR ADVANCED STUDY AND NAGOYA UNIVERSITY.

REFERENCES.

[1] S. Bochner, *Lectures on commutative algebra,* 1938.

[2] E. Cartan, *Les systèmes différentiels extérieurs et leur applications géométriques,* Paris, 1945.

[3] ———, "Sur l'intégration des systèmes d'équations aux différentielles totales," *Annales Scientifiques de l'Ecole Normale Supérieure,* vol. 18 (1901), pp. 241-311.

[4] C. Chevalley, *Theory of Lie groups,* Princeton University Press, 1940.

[5] E. Kähler, "Einführung in die Theorie der Systeme von Differentialgleichungen," *Hamburger Mathematische Einzelschriften,* vol. 16 (1934).

[6] Y. Matsushima, "On a theorem concerning the prolongation of a differential system," *Nagoya Mathematical Journal,* vol. 6 (1953), pp. 1-16.

[7] P. Auslander, "An ideal theory for exterior differential systems," *Annals of Mathematics,* vol. 63 (1956), pp. 527-536.

[8] J. A. Schouten and W. v. d. Kulk, *Pfaff's Problem and its generalization,* Oxford, 1949.

UNIFORM SPACES WITH UNIQUE STRUCTURE.*

By W. F. Newns.

1. It has been proved by A. Weil [10] that a compact space has a unique uniform structure, and by Dieudonné [3] that a completely regular (or even completely normal [4]) space can have a unique structure without being compact. The problem of characterizing spaces with unique structure has been taken up by R. Doss [7], who has given a topological condition for the structure to be unique. It transpired also that a space with a unique structure is necessarily locally compact and that its Alexandroff compactification was the only possible compactification (cf. also [2]). It does not, however, seem to have been pointed out that this last property is *equivalent* to that of having a unique structure, a fact which is not quite obvious since there may conceivably be many structures on a space, but only one in which it is totally bounded.

Theorem 1. *In a completely regular space E, the following properties are equivalent:*

a) *E has a unique uniform structure;*

b) *E has a unique totally bounded uniform structure;*

c) *Of any pair of normally separable closed subsets of E, one at least is compact;*

d) *Each vicinity for each uniform structure on E contains a set of the form $A \times A$, where A is the complement of a compact subset of E.*

Any space having these properties is locally compact, and if not compact its unique compactification is its Alexandroff compactification.

The property c) is the one given by Doss: two closed subsets A and B are said to be normally separable if there exists a continuous mapping f of E into the compact interval $[0,1]$ such that $f(x) = 0$ for $x \in A$ and $f(x) = 1$ for $x \in B$.

If E is compact, the properties are evident, so that we assume henceforth that E is not compact. In this case, the complements of relatively

---

* Received August 16, 1956.

compact subsets of E form a filter, and the property c) is clearly equivalent to:

d′) The filter $\mathcal{F}$ of complements of relatively compact subsets is a Cauchy Filter for every uniform structure on E.

That d′) implies a) has been proved by Dieudonné [3, 291] by observing that any ultrafilter on E must either converge or be finer than $\mathcal{F}$, and hence that any completion of E has just one extra point and is compact, i. e., is the Alexandroff compactification. The property d) is useful in establishing that a given space has a unique structure (cf. [3], and [1, Chap. II, § 4, Exerc. 12]).

It is obvious that a) implies b). To show that b) implies c), let $\mathcal{U}_0$ be the unique totally bounded structure. Since any structure $\mathcal{U}$ on E is finer than some totally bounded structure [1, Chap. IX, § 1, Exerc. 6], it is finer than $\mathcal{U}_0$. Thus $\mathcal{U}_0$ is the coarsest structure on E and is therefore the Alexandroff structure [*ibid.*, Exerc. 11]: the completion $\tilde{E}$ has just one point ω at infinity. Now let A and B be closed subsets of E normally separated by f. Since $\tilde{E}$ is the Stone-Čech compactification of E, f is uniformly continuous in the structure induced on E by that of $\tilde{E}$, and hence extends to $\tilde{E}$. If A is not compact, we have $\omega \in \bar{A}$, so that $f(\omega) = 0$. Thus $\omega \notin \bar{B}$ (otherwise $f(\omega) = 1$) so that B is closed in $\tilde{E}$ and therefore compact.

Since the last part of the theorem has already transpired, it remains only to prove that c) implies d′): i. e., that given any continuous écart f and any $\epsilon > 0$, there exists $A \in \mathcal{F}$ such that $f(x, y) \leqq \epsilon$ whenever $x \in A$ and $y \in A$. Let $V = f^{-1}([0, \epsilon/3])$ and suppose that $V(z)$ is not compact: then since $V(z)$ and the set $\{y : f(y, z) \geqq \epsilon/2\}$ can be normally separated, the latter must be compact, and hence its complement A must belong to $\mathcal{F}$. If x and y are any two points of A we have $f(x, y) \leqq f(x, z) + f(y, z) \leqq \epsilon$ as required. It remains to prove the existence of z. Now if no such z existed, then $V(x)$ would be compact for all $x \in E$, so that E would be complete and paracompact [1, Chap. II, § 4, Exerc. 10], hence normal [6]. But this means that, contrary to hypothesis, E would be compact in view of the following:

A normal space satisfying c) *is countably compact.*

For if not, there would exist in E a sequence (x_n) of distinct points without a limit point. The sets $\{x_{2n}\}$ and $\{x_{2n+1}\}$ would then be closed and disjoint hence normally separable, contrary to c) since neither is compact.

This completes the proof of Theorem 1, so that the result just proved may be stated:

THEOREM 2. *A normal space with a unique structure is countably compact.*

This is, in fact, a special case of a known result [1, Chap. IX, § 4, Exerc. 24] to the effect that a normal space which is totally bounded in all its structures is countably compact. Contrary to a statement by Dickinson [2, Theorem 3], the assumption that the space is normal cannot be omitted from the result. Miss Dickinson showed that the sets $\{x_{2n}\}$ and $\{x_{2n+1}\}$ could be enclosed in disjoint neighbourhoods (without assuming normality) and then asserted that the condition c) is violated (thus implicitly assuming normality). We shall now exhibit a space with a unique structure which is not countably compact.

Let ω, Ω be respectively the first ordinals of the second and third kind, E_0, F_0 the intervals $[1, \omega]$, $[1, \Omega]$ endowed with the open interval topology, and T the complement in $E_0 \times F_0$ of the point (ω, Ω). The space T was first discussed by Tychonoff [8] and has been shown to have a unique structure by Dieudonné [3]. It is clear that T is not countably compact (contrary to [5, § 4]), the sequence $\{(n, \Omega)\}$, for instance, having no limit point. It is easy, moreover, to verify directly that the sets $A = \{(2n, \Omega)\}$ and $B = \{(2n-1, \Omega)\}$ have disjoint neighbourhoods but are not normally separable. Indeed, if V is any neighbourhood of Ω in F_0, the sets $\{n\} \times V$ are mutually disjoint, and suitable unions form the required disjoint neighbourhoods: if f separated A and B, then for each n we could find α_n such that for $x \geqq \alpha_n$ we have $f(n, x) \leqq \frac{1}{4}$ or $f(n, x) \geqq \frac{3}{4}$ according as n is odd or even; if $\alpha < \Omega$ majorised $\{\alpha_n\}$, we should then have $f(n, \alpha) \leqq \frac{1}{4}$ for n odd and $f(n, \alpha) \geqq \frac{3}{4}$ for n even, contrary to the continuity of f at the point (ω, α).

2. It is natural to ask whether the property of having a unique structure is inherited by subspaces. Since frontier points are potential points at infinity, it is the closed subspaces which are most likely to have this property.

THEOREM 3. *A closed subspace of a normal space with a unique structure has itself a unique structure.*

For let A, B be normally separable closed subsets of the closed subspace F of E. Then A and B are closed in E and disjoint, hence normally separable. Since E has a unique structure, either A or B is compact, so that F satisfies the condition c) of Theorem 1 and hence has a unique structure.

A glance at Tychonoff space above will show that the result may fail in non-normal spaces. Indeed, the assumption that E is normal is *necessary.*

THEOREM 4. *If every closed subspace of a completely regular space E has a unique structure, then E is normal.*

For let A be any closed subset of E and f a continuous real-valued function defined on A. The closure $\tilde{A}$ of A in the completion $\tilde{E}$ of E is the completion of A for its unique structure. The function f, being uniformly continuous on A, extends by continuity to $\tilde{A}$; but since $\tilde{E}$ is normal, f may be further extended to $\tilde{E}$, and its restriction to E is then a continuous extension of f from A to E.

A subspace may have a unique structure without being closed, as is shown by regarding a non-compact space with unique structure as a subspace of its compactification. However, it is clear that a subspace with unique structure must either be closed or have a compact closure. In particular, this means that the closure of a subspace with unique structure also has unique structure.

The union of two sets with unique structure need not have a unique structure: the topological sum of two spaces with unique structure (and non-compact) will have two distinct structures, the Stone-Čech compactification providing two points at infinity.

The intersection of two sets with unique structure need not have a unique structure: in the compact space $E_0 \times F_0$ above, the subspace $E_0 \times \{\Omega\}$ is compact, but its intersection with T has not a unique structure.

3. The product of two spaces with unique structure will not in general have a unique structure. Indeed, if a product has a unique structure, then either one of the factors is trivial (i. e., consists of a single point) or both are compact: for let E be non-compact, F non-trivial, E_0, F_0 compactifications of E and F respectively, ω a point at infinity in E_0 and x, y distinct points of F; then $E_0 \times F_0$ is a compactification of $E \times F$ having two distinct points at infinity, namely (ω, x) and (ω, y).

If E is a space with unique structure and R an equivalence relation on E such that E/R is completely regular, then the quotient space will also have a unique structure. This is an immediate corollary of the following result:

THEOREM 5. *Let E be a space with unique structure and f a continuous mapping of E into a completely regular space. Then $f(E)$ has a unique structure.*

For if A, B are closed in $f(E)$ and normally separated by a function g, $f^{-1}(A)$ and $f^{-1}(B)$ are closed in E and normally separated by the function

$g\circ f$. By Theorem 1, one of these sets, say $f^{-1}(A)$, is compact, and hence so is $A=f(f^{-1}(A))$. Applying Theorem 1 again, we see that $f(E)$ has a unique structure.

4. Let E be a space with unique structure, F a completely regular space and f a continuous $(1,1)$ mapping of E onto F. Then if E is compact, so is F, and f is a homeomorphism. *The mapping f will also be a homeomorphism in the case where F (and hence E) is non-compact:* for if F_0 is any compactification of F, f is uniformly continuous as a mapping of E into F_0, hence extends to a mapping $\bar{f}$ of $\tilde{E}$ onto F_0; onto since $\bar{f}(\tilde{E})$ is compact and everywhere dense; since $\tilde{E}$ has just one point at infinity, so has F_0, and $\bar{f}$ is $(1,1)$, hence a homeomorphism.

The case where F is compact but E is not can easily be seen to occur, so that f will not always be a homeomorphism. We need only take E to be a non-compact space with unique structure and F the quotient space obtained by identifying, in $\tilde{E}$, some point of E with the point at infinity. It follows that the topology of a (non-compact) space with unique structure is not a minimal completely regular topology, though all strictly coarser topologies must be compact (cf. [9]).

UNIVERSITY OF LIVERPOOL.

REFERENCES.

[1] N. Bourbaki, *Topologie Generale*, 1940-1949. Paris, Hermann.

[2] A. Dickinson, "Compactness conditions and uniform structure," *American Journal of Mathematics*, vol. 75 (1953), pp. 224-228.

[3] J. Dieudonné, "Sur les espaces uniformes complets," *Annales Scientifiques de l'Ecole Normale Superieure*, vol. 56 (1939), pp. 277-291.

[4] ———, "Un exemple d'espace normal non susceptible d'une structure uniforme d'espace complet," *Comptes Rendus*, vol. 209 (1939), pp. 145-147.

[5] ———, "Sur les espaces topologiques susceptibles d'être munis d'une structure uniforme d'espace complet," *ibid.*, vol. 209 (1939), pp. 666-668.

[6] ———, "Une généralisation des espaces compacts," *Journal de Mathématiques Pures et Appliquées*, New Series, vol. 23 (1944), pp. 65-76.

[7] R. Doss, "On uniform spaces with unique structure," *American Journal of Mathematics*, vol. 71 (1949), pp. 19-23.

[8] A. Tychonoff, "Über die topologische Erweiterung von Raümen," *Mathematische Annalen*, vol. 102 (1930), pp. 544-561.

[9] Jungo Wada, "Lattices of spaces," *Osaka Mathematical Journal*, vol. 5 (1953), pp. 1-5.

[10] A. Weil, *Sur les espaces à structure uniforme*, 1937. Paris, Hermann.

THE CRITERIA FOR ALGEBRAIC EQUIVALENCE AND THE TORSION GROUP.*[1]

By T. Matsusaka.

Let V be a variety in a projective space, non-singular in co-dimension 1. We assume that the reader is familiar with the notion of numerical, algebraic and linear equivalence of divisors, as well as algebraic families of divisors (Weil [14], Chow-v. d. Waerden [2]). Let us denote by $G(V)$, $G_a(V)$ and $G_l(V)$ the groups of V-divisors, V-divisors algebraically equivalent to 0 and V-divisors linearly equivalent to 0 respectively. When V is non-singular, let us denote by $G_n(V)$ the group of V-divisors numerically equivalent to 0. The set of V-divisors X, such that mX is in $G_a(V)$ for a certain positive integer m, forms a group containing $G_a(V)$ and the factor group of it with respect to $G_a(V)$ is called the *torsion group* of V-divisors. By Néron's result (Néron [8]) $G(V)/G_a(V)$ is finitely generated; therefore the torsion group of V-divisors is a finite group. One of the aims of this paper is to show that when V is non-singular, the torsion group is nothing but $G_n(V)/G_a(V)$. We shall prove this directly and we shall not assume Néron's result. Since we need an equivalence criterium for algebraic equivalence, first we shall settle that. This includes, as a special case, the criterium which is formulated in terms of the Poincaré normal function in the classical case of algebraic surfaces (Zariski [16], pp. 128-132).

Let V and V' be two complete non-singular varieties, and f be a birational transformation of V onto V'. Then it is not difficult to see that when Z is a V-divisor such that mZ is algebraically equivalent to 0 on V, $f^{-1}\cdot f(Z) = Z$. The same is true for V'-divisors of the same nature. From this it follows that the torsion group is an absolute invariant of a class of birationally equivalent non-singular complete varieties. But it is not so, when we consider a class of birationally equivalent complete varieties, non-singular in co-dimension 1. For instance, the quotient variety of an Abelian variety A by the group of automorphisms consisting of δ and $-\delta$, which is usually called the *ordinary Kummer variety* of A, is non-singular in co-dimension 1 and has a finite number of singular points; moreover, it is easy to see that it has

---

* Received March 15, 1956; revised October 17, 1956.

[1] This research was supported by the National Science Foundation.

a non-trivial torsion group of divisors. On the other hand, when we desingularize it, we get a complete non-singular variety without a torsion group of divisors, as was shown recently by Spanier (cf. E. Spanier, "The homology of Kummer Manifolds," *Proceedings of the American Mathematical Society*, vol. 7, 1956).

We assume that the reader is familiar with Weil's fundamental works (Weil [12], [13]) and we shall follow the same terminology and conventions. If two divisors X and Y on V are such that $X \equiv Y \bmod G_l(V)$, we shall write $X \sim Y$. We shall denote by $\mathfrak{A}^*$, $\mathfrak{L}^*$ cosets of $G(V)$ modulo $G_a(V)$ and $G_l(V)$ respectively. If $\mathfrak{A}^*$ or $\mathfrak{L}^*$ contains a divisor X, we shall write sometimes $\mathfrak{A}^*(X)$ or $\mathfrak{L}^*(X)$ for $\mathfrak{A}^*$ or $\mathfrak{L}^*$. In the same way, when V is non-singular, we shall denote by $\mathfrak{N}^*$ a coset of $G(V)$ modulo $G_n(V)$ and when it contains a divisor X, we shall write $\mathfrak{N}^*(X)$ for $\mathfrak{N}^*$. We shall denote by $\mathfrak{N}, \mathfrak{A}, \mathfrak{L}$ (resp. $\mathfrak{N}(X), \mathfrak{A}(X), \mathfrak{L}(X)$) the sets of positive divisors in $\mathfrak{N}^*, \mathfrak{A}^*, \mathfrak{L}^*$ (resp. $\mathfrak{N}^*(X), \mathfrak{A}^*(X), \mathfrak{L}^*(X)$). It is well-known that $\mathfrak{L}$ is an algebraic family, usually known as a *complete linear system.* Let X be a V-divisor and $L(X)$ be the module of rational functions f on V such that $(f) \succ -X$. We shall denote by $l(X)$ the dimension of $L(X)$ over the universal domain, which is $\dim \mathfrak{L}(X) + 1$, where $\dim \mathfrak{L}(X)$ means the dimension of $\mathfrak{L}(X)$ as an algebraic family, i.e. the smallest dimension of varieties which parametrize $\mathfrak{L}(X)$.

Let Y be a positive cycle in a projective space. Regarding the set of coefficients of the Chow-form (Zugeordnete Form) of Y, arranged in a certain order, as a set of homogeneous coordinates of a point, we call it the *Chow-point* of Y. If an integer d is given, the set of all positive V-divisors of degree d forms a finite set of algebraic families (Chow-v. d. Waerden [2]). Each such family is called a *maximal algebraic family* since it is not contained in another family consisting of positive divisors of the same degree. An algebraic family $\mathfrak{F}$ is called *total,* if for any V-divisor Z algebraically equivalent to 0, there is a divisor X in $\mathfrak{F}$ such that $Z \sim X - X_0$, for a fixed divisor X_0 in $\mathfrak{F}$ (Matsusaka [3], Th. 1). We shall say that an algebraic family is defined over a field K, if its Chow-variety (i.e. the set of corresponding Chow-points) is defined over K. About maximal algebraic families, we know the following results.

THEOREM 1. *Let V be a projective variety, non-singular in co-dimension* 1, *and C be a hyperplane section of V.* (i) *For a given divisor X, there is a positive integer m_0 such that whenever $m \geqq m_0$, there is a total maximal family in $\mathfrak{A}(X + mC)$.* (ii) *If $\mathfrak{F}$ and $\mathfrak{F}'$ are two total maximal families of* *divisors on V in the same coset $\mathfrak{A}^*$, then $\mathfrak{F}=\mathfrak{F}'$.* (iii) *Assume that V is non-singular. If a V-divisor X is given, there is a positive integer m_0 having the following properties: whenever $m \geqq m_0$, $\mathfrak{A}(X+mC)$ itself is a total algebraic family; any two divisors in $\mathfrak{A}(X+mC)$ determine complete linear systems of the same dimension; and for any divisor Y in $\mathfrak{A}(X+mC)$, $\mathfrak{L}(Y)$ contains a non-singular variety.*

For these, see Matsusaka [5], Th. 2, Lemma 2.

We can define *specializations of cycles* on projective varieties. Specializations are compatible with the operations of addition, multiplication and algebraic projection. As far as positive cycles are concerned, specializations are compatible with the operation of intersection-product. Moreover, when the ambient variety is non-singular in co-dimension 1, algebraic equivalence and linear equivalence of divisors are preserved by specializations. For the general treatment of specializations, we refer to Shimura [10]. We shall write $X \rightarrow X'$ ref k, when a cycle X' is a specialization of a cycle X with reference to k.

Let V be a variety defined over a field k in a projective space and $H_1, \cdots, H_s$ be s independent generic hypersurfaces in the ambient space over k. Then $V \cdot H_1 \cdot \cdot \cdot H_s$ is defined and is a variety; and it is non-singular (resp. non-singular in co-dimension 1) when V is non-singular (resp. non-singular in co-dimension 1) (Weil [14]). Let us call it a *general variety on V generic over k.* When we say that a variety W is a general variety on V, it is understood that W is a general variety on V, generic over a certain field of definition for V.

1. Let us fix once for all a projective variety V, non-singular in co-dimension 1 and an *algebraically closed* field of defintion k of V. We regard k as a basic field and all fields will be assumed to contain k.

LEMMA 1. *Let W be a general variety on V generic over k and K be a common field of definition for V and W. Let X and X' be V-divisors such that $X \rightarrow X'$* ref K *and that $X \cdot W$ is defined. When*

$$(1) \quad (X, X\cdot W) \rightarrow (X', Y) \text{ ref } K, \qquad (2) \quad (X, X\cdot W) \rightarrow (X', Y^*) \text{ ref } K,$$

are two specializations of $(X, X\cdot W)$ over $X \rightarrow X'$ ref K, *then Y and Y^* are linearly equivalent on W.*[2]

Proof. First let us consider the case when X is positive . Then X' is also positive. We can find projecting cones R and R' of X and X' respectively such that

---

[2] The writer wishes to take this opportunity to correct the error in the proof of Prop. 2, Matsusaka [3]. Prop. 2 itself is an immediate consequence of this lemma.

$$R\cdot V=X+N,\ R'\cdot V=X'+N',\ \deg(R)=\deg(R')=\deg(X)=\deg(X'),$$

that $N\cdot W$, $N'\cdot W$ are both defined and that R' is the uniquely determined specialization of R over the specialization $X\to X'$ ref K (for projecting cones, see v. d. Waerden [11], pp. 634-635). Let H be a hypersurface of the same degree as R defined over K such that $H\cdot V$ and $H\cdot W$ are both defined. We have $X\sim H\cdot V-N$, $X'\sim H\cdot V-N'$. By the compatibility of specializations with the operation of intersection-product, $X\to X'$ ref K determines uniquely the specialization $(X,N,N\cdot W)\to(X',N',N'\cdot W)$ ref K. Hence (1) and (2) determine uniquely specializations

$$(1')\qquad (X,X\cdot W,N,N\cdot W)\to(X',Y,N',N'\cdot W)\text{ ref }K,$$

$$(2')\qquad (X,X\cdot W,N,N\cdot W)\to(X',Y^*,N',N'\cdot W)\text{ ref }K.$$

Since linear equivalence is preserved by specializations and since $X\cdot W\sim H\cdot W-N\cdot W$, we get, from (1′) and (2′), the following relations: $X\sim H\cdot W-N'\cdot W$, $Y^*\sim N\cdot W-N'\cdot W$. This proves our lemma in the case when X is positive.

Suppose that X is not positive and write $X=X_1-X_2$, $X_i\succ 0$ for $i=1,2$. Let

$$(X,X\cdot W,X_1,X_2,X_1\cdot W,X_2\cdot W)\to(X',Y,X_1',X_2',Z_1,Z_2)\text{ ref }K,$$

$$(X,X\cdot W,X_1,X_2,X_1\cdot W,X_2\cdot W)\to(X',Y^*,X_1',X_2',Z_1^*,Z_2^*)\text{ ref }K,$$

be extensions of (1) and (2) respectively. We have $X'=X_1'-X_2'$ and by what we have seen already in the case of positive divisors, $Z_1\sim Z_2^*$, $Z_2\sim Z_2^*$. Since $X\cdot W=X_1\cdot W-X_2\cdot W$, we have $Y=Z_1-Z_2$ and $Y^*=Z_1^*-Z_2^*$, which prove that $Y\sim Y^*$. Thus our lemma is proved.

LEMMA 2. *Let U be a variety in a projective space L_1 and f be a rational mapping of U into a projective space L_2 such that f is everywhere single-valued. Let X be a subvariety of U and X' be a specialization of X over a common field of definition K for U and f. If the image of X by f is a d-dimensional variety, there is a component of X' such that its image by f has at least dimension d.*

Proof. It is clear that if our lemma is true when U is a normal variety, it is true in general, by passing from the given variety to its derived normal variety. Therefore, let us assume that U is a normal variety. Let Z be the graph of f. By our assumption, f is everywhere defined on U. There is a uniquely determined subvariety X^* of Z of the same dimension as X with the projection X on U (Weil [12], Chap. 4, Th. 15). Let $(X, X^*) \to (X', Y)$ ref K be an extension of $X \to X'$ ref K on $L_1 \times L_2$. By the compatibility of specializations with the operation of algebraic projection, we see that $\mathrm{pr}_1 Y = X'$, where pr_1 is the operation of algebraic projection on the first factor of the product $L_1 \times L_2$. Hence if $X' = \sum a_i Z_i$ is the reduced expression for X', $Y = \sum a_i Z_i^*$ is the reduced expression for Y, where Z_i^* is the uniquely determined subvariety of Z with the projection Z_i on U.

Let H be a generic linear variety of co-dimension d in L_2 over a field over which X, X' are both rational and $K(u)$ be the smallest field of definition for H containing K. Then $(X, X^*) \to (X', Y)$ ref $K(u)$ on $L_1 \times L_2$. Since $X^* \cdot (L_1 \times H)$, $Y \cdot (L_1 \times H)$ are both defined (Weil [12], Chap. 5, Prop. 2), we see that $X^* \cdot (L_1 \times H) \to Y \cdot (L_1 \times H)$ ref $K(u)$ on $L_1 \times L_2$. Because of the fact that the former is not empty, the latter cannot be empty. This proves our lemma.

LEMMA 3. *Assume that V is normal and let X be a positive V-divisor. Let K be a field of definition for V over which X is rational and let C be a hyperplane section of V, generic over K. There is a positive integer h_0 such that whenever $h \geqq h_0$, the complete linear system $\mathfrak{L}(X + hC)$ induces a complete linear system on C.*

This is the so-called Castelnuovo lemma in the classical case. As to the proof, see Matsusaka [5], p. 126.

2. Let us recall some of the known results on Picard varieties which we shall need later. Let U be a complete algebraic variety, non-singular in co-dimension 1 and K be a field of definition for U. Let G be a subset of $G(U)$ and f be a mapping of G into an algebraic variety W with the following properties: (i) f is defined outside of a proper subset of G; (ii) there is a common field of definition K' for U and W such that when Z is a divisor in G, rational over a field K^* containing K', $f(Z)$ is rational over K^* if it is defined. When f satisfies the above conditions, then we shall say that f is a *rational mapping* of G and K' is a *field of definition* of f. Moreover, if G is a subgroup of $G(U)$, W a group variety and f a group-homomorphism, we shall say that f is a *rational homomorphism.* There is an Abelian variety P and a rational homomorphism f of $G_a(U)$ onto P such that the kernel of f is $G_l(U)$ and that f has the universal mapping property as a rational homomorphism of $G_a(U)$ into an Abelian variety. P is called the

Picard variety of U and f is called the *canonical homomorphism* of $G_a(U)$ onto P. When U is a projective variety, we may take P, f to be defined over K and when $\dim U > 2$, the Picard variety of U and the Picard variety of a general variety on U of dimension at least 2 differ by a purely inseparable homomorphism. As to these, see Chow [1]; Matsusaka [3], [4], [6], [7]; Néron-Samuel [9].

Let us asume, from now on, that V is a *normal variety*. Let W be a general variety on V generic over k and $k(u)$ be the smallest field of definition for W. Then $k(u)$ is a purely transcendental extension of k. We regard (u) as a parameter on which W depends over the field k, and we shall write sometimes W_u for W. W is a normal variety since V is normal (Zariski [15], Th. 3). Let us denote by $P(V)$ and $P(W)$ the Picard varieties of V and W. Then as we have remarked already, we may assume that $P(V)$, $P(W)$ are defined over k and over $k(u)$ respectively, together with the canonical homomorphisms. Let $\mathfrak{F}$ be an algebraic family of positive V-divisors defined over a field K and assume that W_u is a general variety on V generic over K. Let X be a generic divisor of $\mathfrak{F}$ over $K(u)$; then $X \cdot W_u$ is defined and is rational over a regular extension of $K(u)$. Let $\mathfrak{F}'$ be the set of specializations of $X \cdot W_u$ over $K(u)$, which we shall call the *family induced on* W_u *by* $\mathfrak{F}$.

LEMMA 4. *Let $\mathfrak{F}$ and $\mathfrak{F}^*$ be two total maximal families of positive V-divisors and W_u be a general variety generic over a common field K of definition for $V, \mathfrak{F}$ and $\mathfrak{F}^*$. Let X and X^* be generic divisors of $\mathfrak{F}$ and $\mathfrak{F}^*$ over $K(u)$ and assume that $\mathfrak{L}(X)$, $\mathfrak{L}(X^*)$ induce again on W_u complete linear systems.* (i) *If $\dim W_u = 1$ and if the induced families $\mathfrak{F}'$, $\mathfrak{F}^{*\prime}$ contain W_u-divisors linearly equivalent to each other on W_u, then $\mathfrak{F}'$ and $\mathfrak{F}^{*\prime}$ coincide.* (ii) *If $\dim W_u > 1$ and if $\mathfrak{F}'$ and $\mathfrak{F}^{*\prime}$ contain divisors algebraically equivalent to each other on W_u, then $\mathfrak{F}'$ and $\mathfrak{F}^{*\prime}$ coincide.*

Proof. According to Weil's equivalence criteria for linear equivalence (Weil [14], Cor. 2, Th. 7), any V-divisor Z such that $Z \cdot W_u \sim 0$ on W_u is linearly equivalent to 0 on V, provided Z is algebraically equivalent to 0. Let us omit to write u and let $P(W)$ and f be the Picard variety of W and the canonical homomorphism of $G_a(W)$ onto $P(W)$, both defined over $K(u)$. Let us assume that $\dim W = 1$; let Y and Y^* be W-divisors contained in $\mathfrak{F}', \mathfrak{F}^{*\prime}$ which are linearly equivalent to each other on W and T, T^* be the loci of $f(X \cdot W - Y)$, $f(X^* \cdot W - Y^*)$ over the algebraic closure of $K(u)$ respectively. Then T and T^* are Abelian varieties in $P(W)$ and $T = T^*$ since $\mathfrak{F}$ and $\mathfrak{F}^*$ are maximal total families. T is isogenous to the Picard variety $P(V)$ of V (in fact, differs from $P(V)$ by a purely inseparable homomorphism) by Weil's equivalence criteria for linear equivalence. Let x be a generic point of T over the algebraic closure K' of $K(u)$. Then by the main theorem on Jacobian varieties (Weil [13], Th. 19), there is a positive W-divisors Z of the same degree as Y, Y^* such that $f(Z-Y)=x=f(Z-Y^*)$. Let X_1 and $X_1{}^*$ be generic divisors of $\mathfrak{F}$ and $\mathfrak{F}^*$ over $K(u)$ such that $f(X_1\cdot W-Y)=x=f(X_1{}^*\cdot W-Y^*)$. Then $X_1\cdot W\sim X_1{}^*\cdot W\sim Z$. By our assumption, $\mathfrak{L}(X_1), \mathfrak{L}(X_1{}^*)$ induce on W complete linear systems. Therefore, $\mathfrak{L}(X_1)=\mathfrak{L}(X_1{}^*)=\mathfrak{L}(Z)$ and $\mathfrak{L}(Z)$ is contained in both $\mathfrak{F}'$ and $\mathfrak{F}^{*\prime}$. Let K^* be a field of definition for the algebraic family $\mathfrak{L}(Z)$ containing K' and Z^* be a generic divisor of $\mathfrak{L}(Z)$ over K^*. Then $X_1\cdot W$ and $X_1{}^*\cdot W$ are specializations of Z^* over K^* and, a fortiori, over K'. This proves (i) when we take the definition of induced families into account.

Assume that $\dim W>1$. The same equivalence criteria of Weil show that $\mathfrak{F}'$ and $\mathfrak{F}^{*\prime}$ are total families on W since $P(V)$ and $P(W)$ have the same dimension in this case (Chow [1], Matsusaka [7]). By our assumption, $\mathfrak{F}', \mathfrak{F}^{*\prime}$ contain divisors Y and Y^* which are algebraically equivalent to each other on W. Hence $\mathfrak{F}'$ and $\mathfrak{F}^{*\prime}$ coincide by Th. 1, (ii), provided both are maximal families. But since generic divisors of $\mathfrak{F}$ and $\mathfrak{F}^*$ over $K(u)$ are such that the complete linear systems determined by them induce on W complete linear systems by our asumption, $\mathfrak{F}'$ and $\mathfrak{F}^{*\prime}$ must be maximal. Our lemma is thereby proved.

PROPOSITION 1. *Let $\mathfrak{F}$ and $\mathfrak{F}^*$ be two total families on V; let K be an algebraically closed common field of definition for V, $\mathfrak{F}$ and $\mathfrak{F}^*$; let W_u be a general variety on V generic over K and $\mathfrak{F}'$, $\mathfrak{F}^{*\prime}$ be the families induced on W_u by $\mathfrak{F}$ and $\mathfrak{F}^*$ respectively. Assume that $\mathfrak{F}'=\mathfrak{F}^{*\prime}$.* (i) *When* $\dim W_u=1$, *there is a finite set of subvarieties $D_1,\cdots,D_s$ of V depending only upon W_u such that if X and X^* are divisors in $\mathfrak{F}$ and $\mathfrak{F}^*$ respectively, $X-X^*$ is algebraically equivalent to a linear combination $\sum m_iD_i$ of the D_i. The D_i have the property that $\sum a_iD_i\equiv 0 \bmod G_a(V)$ if and only if $a_i=0$.* (ii) *When* $\dim W_u>1$, *$\mathfrak{F}$ and $\mathfrak{F}^*$ belong to the same coset of $G(V) \bmod G_a(V)$.*

When $\mathfrak{F}$ and $\mathfrak{F}^*$ are both maximal and total, then $\mathfrak{F}=\mathfrak{F}^*$ if every $m_i=0$ in the case when $\dim W_u=1$. *$\mathfrak{F}=\mathfrak{F}^*$ when* $\dim W_u>1$.

Proof. Let X and X^* be generic divisors of $\mathfrak{F}$ and $\mathfrak{F}^*$ respectively over $K(u)$ and C be a hyperplane section of V rational over K. By using our Lemma 3, we see that when m is sufficiently large, $\mathfrak{L}(X+mC)$ and $\mathfrak{L}(X^*+mC)$ again induce on W_u complete linear systems. Let $\mathfrak{F}_1$ and $\mathfrak{F}_1{}^*$ be maximal families containing $X+mC$ and X^*+mC respectively as members. Then it is easy to see that $\mathfrak{F}_1$ and $\mathfrak{F}_1{}^*$ are both maximal total families and by our assumption the induced families $\mathfrak{F}_1{}'$ and $\mathfrak{F}_1{}^{*\prime}$ contain common W_u-divisors. By our choice of X, X^* and C, $X+mC$ and X^*+mC are linearly equivalent to generic divisors of $\mathfrak{F}_1$ and $\mathfrak{F}^*$ respectively over $K(u)$. Therefore, $\mathfrak{F}_1'$ and $\mathfrak{F}_1^{*\prime}$ coincide by Lemma 4. If (i) and (ii) are true for $\mathfrak{F}_1$ and $\mathfrak{F}_1^*$, they are also true for $\mathfrak{F}$ and $\mathfrak{F}^*$. Hence let us assume that $\mathfrak{F}$ and $\mathfrak{F}^*$ are both total and maximal.

Let U and U^* be the Chow-varieties of $\mathfrak{F}$ and $\mathfrak{F}^*$ (the set of Chow-points of divisors in $\mathfrak{F}$ and $\mathfrak{F}^*$) and x, x^* be the Chow-points of X, X^*. Let h_u, h_u^*, g_u be the rational mappings from U, U^* and from $U \times U^*$ defined as follows:

$$h_u(x) = f_u((X - X_0) \cdot W_u)\,; \qquad h_u^*(x^*) = f_u((X^* - X_0) \cdot W_u)\,;$$
$$g_u(x \times x^*) = f_u((X - X^*) \cdot W_u),$$

where X_0 is a fixed rational divisor in $\mathfrak{F}$ over K and f_u is the canonical homomorphism of $G_a(W_u)$ onto $P(W_u)$. Since W_u is defined over $K(u)$, we may assume that $P(W_u)$ and f_u are both defined over $K(u)$. Of course, the second and third formulas have a meaning by our assumption; $h_u(x)$ and $h_u^*(x^*)$ have the same locus A_u over $K(u)$, which is an Abelian variety on $P(W_u)$ and differs from the Picard variety $P(V)$ of V by a purely inseparable homomorphism. Let us observe that h_u, h_u^* and g_u are everywhere single-valued rational mappings defined over $K(u)$; this is an immediate consequence of our Lemma 1.

Let 0_u be the neutral element of $P(W_u)$ as a group, which is also the same for the group A_u. Let us prove that $g_u^{-1}(0_u)$ contains a component Z_u defined over a purely inseparable extension of $K(u)$ such that when $y \times y^*$ is a generic point of Z_u over the algebraic closure of $K(u)$, y and y^* are generic points of U and U^* over $K(u)$. We have $g_u(x \times x^*) = h_u(x) - h_u^*(x^*)$ and hence $g_u^{-1}(0_u)$ consists of points $y' \times y^{*\prime}$ such that $h_u(y') = h_u^*(y^{*\prime})$. Let us put $h_u(x) = w$. It is not difficult to see that $h_u^{-1}(w)$ consists of Chow-points of divisors contained in $\mathfrak{L}(X)$ by Weil [12], Chap. 6, Th. 11 and by the criteria for linear equivalence. Let y^* be a generic point of U^* over $K(u)$ such that $h_u^*(y^*) = w$ and Y^* be the divisor in $\mathfrak{F}^*$ with the Chow-point y^*. Then again $h_u^{*-1}(w)$ consists of Chow-points of divisors in $\mathfrak{L}(Y^*)$. Therefore, the point sets $|h_u^{-1}(w)|$, $|h_u^{*-1}(w)|$ are the point sets of Chow-varieties of $\mathfrak{L}(X), \mathfrak{L}(Y^*)$ respectively. Let us assume that x and y^* are independent generic points of $|h_u^{-1}(w)|$, $|h_u^{*-1}(w)|$ over the algebraic closure of $K(u, w)$; let Z_u be the locus of $x \times y^*$ over the algebraic closure of $K(u)$. We see that Z_u is contained in a component of $g_u^{-1}(0_u)$ and x, y^* are generic points of U, U^* over $K(u)$. Let T be a component of $g_u^{-1}(0_u)$ containing Z_u and $t \times t^*$ be a generic point of T over the algebraic closure of $K(u)$. Then $h_u(t) = h_u^*(t^*) = w'$ is a generic point of A_u over $K(u)$ and is a generic specialization of w over the algebraic closure of $K(u)$. Therefore, by our choice of x, y^*, $t \times t^*$ must be a generic specialization of $x \times y^*$ over the algebraic closure of $K(u)$. This proves that $T = Z_u$. Now let $(Z_u', x', y^{*\prime})$ be a generic specialization of (Z_u, x, y^*) over $K(u)$. Then $h_u(x') = h_u^*(y^{*\prime}) = w'$ is a generic specialization of w over $K(u)$. Since A_u is defined over $K(u)$, it follows that w' is also a generic specialization of w over the algebraic closure of $K(u)$. Therefore $(w, h_u^{-1}(w), h_u^{*-1}(w))$ is a generic specialization of $(w', h_u^{-1}(w'), h_u^{*-1}(w'))$ over the algebraic closure of $K(u)$. This shows that Z_u and Z_u' coincide by the definition of Z_u. Thus our assertion is proved.

Now we are in position to prove our proposition. Let $\mathfrak{S}$ be the set of specializations of Z_u over K in the ambient space of $U \times U^*$; $\mathfrak{S}$ is an algebraic family of varieties defined over K and Z_u is a generic variety of it over K. Let u' be an independent generic specialization of u over K, then $Z_{u'}$ is also a generic variety of $\mathfrak{S}$ over K. Moreover, $Z_{u'}$ is also a generic variety of $\mathfrak{S}$ over $K(u)$ and consequently Z_u is a specialization of $Z_{u'}$ over $K(u)$. Since g_u is everywhere single-valued and since Z_u is such that every point on it is mapped to one and the same point 0_u, it follows that every point on $Z_{u'}$ is mapped also to one and the same point by g_u according to Lemma 2. Let us denote such a point on $P(W_u)$ by $Q(u')$. Since $Z_{u'}$ is defined over a purely inseparable extension of $K(u')$, there is a positive integer m such that it is defined over $K(u'^{p^{-m}})$, where $K(u'^{p^{-m}})$ is the image of $K(u')$ by the automorphism of the universal domain defined by $z \rightarrow z^{p^{-m}}$. Let R be the locus of $v' = u'^{p^{-m}}$ over K, which is a rational variety since $K(u')$ is a purely transcendental extension of K. Put $v = u^{p^{-m}}$. We get a rational mapping f from R into $P(W_u)$ defined over $K(u)$ such that $f(v') = Q(u')$ and that $(v, Q(u))$ is a specialization of $(v', Q(u'))$ over $K(u)$. On the other hand, every rational mapping from a rational variety into an Abelian variety is a constant by Weil [13], Cor., Th. 8. Hence $f(v') = Q(u') = 0_u$ and from this we see that $(X - Y^*) \cdot W_u \sim 0$ on W_u. Therefore, when $\dim W_u > 1$, $X \sim Y^*$ and when $\dim W_u = 1$, $X - Y^* \sim \sum m_i D_i$ where the D_i are subvarieties of V having the properties stated in our proposition (Weil [14], Cor., Prop. 5). Thus we have proved (i) and (ii). The rest of our assertion follows from Theorem 1.

Let C be a general curve on V generic over k, J be the Jacobian variety of C and ϕ be the canonical function of C into J. Let us associate to every positive V-divisor X the point

$$S(\phi(C \cdot X)) = f(X),$$

which is the sum of the components of $C\cdot X$ on J. In the case when $C\cdot X$ is not defined, let Y be a divisor linearly equivalent to X such that $C\cdot Y$ is defined, then we define $f(X)=f(Y)$. This definition is compatible with specializations by Lemma 1.

Let $\mathfrak{F}$ be a total family on V defined over k and X_0 be a fixed rational divisor in $\mathfrak{F}$ over k. When X is a generic divisor of $\mathfrak{F}$ over a common field of definition K for C, J and $\phi, f(X)-f(X_0)$ has a locus A over K which is an Abelian variety in J, and differs from the Picard variety of V by a purely inseparable homomorphism. Let us prove the following theorem.

THEOREM 2. *Let C, J, ϕ, A be as described and Y, Y' be two positive divisors of the same degree on V. Let $D_1,\cdots,D_s$ be subvarieties of V with the properties stated in Prop. 1. If Y and Y' are algebraically equivalent to each other, $f(Y)$ and $f(Y')$ differ by a point of A. Conversely, when $f(Y)-f(Y')$ is a point of A, $Y-Y'$ is algebraically equivalent to a linear combination of $D_1,\cdots,D_s$.*

Proof. Suppose that $Y-Y'$ is algebraically equivalent to 0. Let $\mathfrak{F}$ be a total family on V and X_0 be a fixed divisor in $\mathfrak{F}$. There is a divisor X in $\mathfrak{F}$ such that $Y-Y'\sim X-X_0$. Hence $f(Y)=f(Y')=f(X)-f(X_0)$ which is a point on A. Therefore, we get the first assertion.

Let W be a hyperplane section of V and let us take m so large that there are total maximal families $\mathfrak{G}, \mathfrak{G}'$ such that $\mathfrak{G}$ is contained in $\mathfrak{A}(Y+mW)$ and $\mathfrak{G}'$ is contained in $\mathfrak{A}(Y'+mW)$ (cf. Th. 1.). Let K be an algebraically closed common field of definition for $V, C, J, \phi, A, \mathfrak{F}, \mathfrak{G}, \mathfrak{G}'$ and Z and Z' be generic divisors of $\mathfrak{G}$ and $\mathfrak{G}'$ over K. By the Lemma 3, we may assume that $\mathfrak{L}(Z)$ and $\mathfrak{L}(Z')$ induce on C complete linear systems. Since $\mathfrak{G}$ and $\mathfrak{G}'$ are total, the loci of $f(Z), f(Z')$ over K are of the form $A_b, A_{b'}$. Our assumption shows that $f(Y+mW)=f(Y'+mW)+a$ where a is a point on A. Hence $A_b, A_{b'}$ have a point in common, and consequently $A_b=A_{b'}$. On the other hand, since $\mathfrak{L}(Z)$ and $\mathfrak{L}(Z')$ induce on C complete linear systems, $\mathfrak{G}$ and $\mathfrak{G}'$ induce on C the same algebraic family, as can be seen easily by using the fundamental theorem on Jacobian varieties (Weil [13], Th. 19). Then our assertion follows from Prop. 1.

Remark. It is very desirable to eliminate the subvarieties $D_1,\cdots,D_s$ from our theorem. In order to do so, we have to eliminate them from Weil's equivalence criteria. In particular, we have to do so for Weil [13], Th. 2. Suppose that W is a general surface on V generic over k. Assume that W has the property that the generic linear pencil contained in the linear system of hyperplane sections on W does not contain reducible members. Let H be a generic hyperplane with respect to V and W and take $W \cdot H$ to be a general curve on V generic over k. Then we can eliminate those special subvarieties from the equivalence criteria for linear equivalence and our theorem becomes as follows.

The necessary and sufficient condition that Y and Y' are algebraically equivalent is that $f(Y)$ and $f(Y')$ differ by a point of A.

Those algebraic surfaces which do not fulfill the above mentioned property are known to be the *ruled surfaces* or the *Steiner surfaces* in the classical case. But this difficulty may be avoided by applying a birational transformation to V. In fact, there is a normal projective variety V', birationally equivalent to V, such that a general surface on V' has the above mentioned property (cf. Néron-Samuel [9], §4).

THEOREM 3. *Let W be a general variety on V generic over k; let Z be a V-divisor such that $Z \cdot W$ is defined. When* $\dim W \geqq 2$ *and $Z \cdot W$ is algebraically equivalent to* 0 *on W, Z is algebraically equivalent to* 0 *on V.*

Proof. Let us write Z as the difference $X - X^*$ of two positive divisors. Since we are interested in algebraic equivalence, we may replace Z by another V-divisor algebraically equivalent to Z. In particular, we may assume that Z is rational over k since k is algebraically closed. Let C be a hyperplane section of V, rational over k and let $\mathfrak{F}$ and $\mathfrak{F}^*$ be total maximal families contained in $\mathfrak{A}(X + mC)$ and $\mathfrak{A}(X^* + mC)$ for sufficiently large m (cf. Th. 1). By Lemma 3, we may assume that the complete linear systems determined by generic divisors of $\mathfrak{F}$ and $\mathfrak{F}^*$ over a common field K of definition for V and W induce on W complete linear systems, by taking m sufficiently large. Our assumption shows that the induced families $\mathfrak{F}'$ and $\mathfrak{F}^{*\prime}$ on W by $\mathfrak{F}$ and $\mathfrak{F}^*$ contain divisors algebraically equivalent to each other on W. Therefore, by Lemma 4, (ii), $\mathfrak{F}'$ and $\mathfrak{F}^{*\prime}$ coincide and consequently $\mathfrak{F}$ and $\mathfrak{F}^*$ coincide by Prop. 1. This proves that Z is algebraically equivalent to 0.

3. Let us assume here that V is a *non-singular algebraic surface.*

PROPOSITION 2. *Let X and X' be V-divisors numerically equivalent to each other. Then the virtual arithmetic genus $p_a(X)$ of X and that of X' coincide* (for the definition of the virtual arithmetic genus, see Zariski [15]).

Proof. Let $K(V)$ be a canonical divisor of V. Let us assume first that X and X' are both non-singular curves. Since $\mathfrak{L}(X + K(V))$ induces on X a linear system contained in the canonical system (Zariski [15], §13), we have

$$\deg(X \cdot (X + K(V))) = 2g(X) - 2, \qquad \deg(X' \cdot (X' + K(V))) = 2g(X') - 2,$$

where $g(X), g(X')$ denote the genera of X, X'. Since X and X' are numerically equivalent to each other, we see, from the above formulas, that $g(X) = g(X')$. Consequently we get the equality $p_a(X) = p_a(X')$ since the virtual arithmetic genus of a non-singular curve and its genus coincide. In the general case, let C be a hyperplane section of V. When m is sufficiently large, $\mathfrak{L}(X + mC)$ and $\mathfrak{L}(X' + mC)$ contain non-singular curves (Matsusaka [5], Lemmas 1, 2). Since all divisors in the same coset of $G(V)$ mod $G_l(V)$ have the same virtual arithmetic genus (Zariski [15], Lemma 4), we get the following equality by using the so-called modular property of p_a.

$$p_a(X) + p_a(mC) + p_a(mX \cdot C) = p_a(X') + p_a(mC) + p_a(mX' \cdot C).$$

(cf. Zariski [15], p. 582).

By the definition of p_a, we have $p_a(mX \cdot C) = \deg(mX \cdot C) - 1$ and $p_a(mX' \cdot C) = \deg(mX' \cdot C) - 1$. Therefore, we get the equality $p_a(X) = p_a(X')$.

PROPOSITION 3. *$G_n(V^2)/G_a(V^2)$ is a finite group.*

Proof. Let $\mathfrak{F}$ be a maximal total family on V such that it contains a divisor X satisfying the inequalities

$$\deg(X \cdot X) - p_a(X) + p_a(V) + 1 \geqq 0, \quad \deg(X) > \deg(K(V)).$$

When we take $\mathfrak{F}$ to be a maximal total family contained in $\mathfrak{A}(mX)$, where mC is a sufficiently high multiple of a hyperplane section C of V, the above condition is satisfied (cf. Th. 1 and Zariski [15], § 14). By the main theorem in Chow-v. d. Waerden [2], there is a finite number of maximal families of divisors $\mathfrak{F}_1 = \mathfrak{F}, \cdots, \mathfrak{F}_m$ in $\mathfrak{N}(X)$ such that any divisor in $\mathfrak{N}(X)$ is algebraically equivalent to a divisor in $\mathfrak{F}_i$ for some i, but no two of the $\mathfrak{F}_i$'s contain divisors algebraically equivalent to each other. Let X_i be a divisor in $\mathfrak{F}_i$ and assume that $X_1 = X$. By our assumption, X_i and X_j are algebraically equivalent to each other if and only if $i = j$. Let Z be any divisor numerically equivalent to 0. Then $X + Z$ and X are numerically equivalent to each other. Hence both have the same self-intersection number and the same virtual arithmetic genus by Prop. 2. Moreover, since $\deg(K(V)) < \deg(Z + X)$, it follows that $l(K(V) - X - Z) = 0$. Hence

$$\deg((X + Z) \cdot (X + Z)) - p_a(X + Z) + p_a(V) + 1 \geqq 0.$$

By the theorem of Riemann-Roch (Zariski [15], § 14), we see that $\mathfrak{L}^*(X + Z)$ contains a positive divisor X'. Hence X' must be algebraically equivalent to one of the X_i's. This proves that $X_i - X$ $(i = 1, \cdots, m)$ gives a complete set of representatives of $G_n(V)$ mod $G_a(V)$. Our proposition is thereby proved.

4.

THEOREM 4.[3] *Let V be a non-singular projective variety. Then $G_n(V)/G_a(V)$ is a finite group, and consequently it is the torsion group of V-divisors.*

Proof. Let W be a general surface on V and let r be the order of the group $G_n(W)/G_a(W)$. Assume that $G_n(V)/G_a(V)$ contains more than r elements and let $Z_1, \cdots, Z_{r+1}$ be $r+1$ representatives of $G_n(V) \bmod G_a(V)$ such that $Z_i \not\equiv Z_j \bmod {}_a(V)$ for $i \neq j$. We may assume that $Z_i \cdot W$ is defined. By Theorem 3, $\sum a_i Z_i \cdot W \equiv 0 \bmod G_a(W)$ implies $\sum a_i Z_i \equiv 0 \bmod G_a(V)$, but we must have a relation of the form $Z_i \cdot W \equiv Z_j \cdot W \bmod G_a(W)$ for a certain pair (i, j) of indices. This is impossible by our choice of the Z_i and consequently $G_n(V)/G_a(V)$ contains at most r elements. From this our theorem follows immediately.

Let $Z_1, \cdots, Z_s$ be a complete set of representatives of $G_n(V) \bmod G_a(V)$ and C be a hyperplane section of V. When m is sufficiently large, $\mathfrak{L}^*(Z_i + mC)$ contains a divisor $X_i \succ 0$ for every i. Let us assume that Z_i is algebraically equivalent to 0. Then X_1 is algebraically equivalent to mC. Thus we get the following corollary.

COROLLARY. *Let V be a projective non-singular variety and X be a positive V-divisor such that $\mathfrak{L}(X)$ determines an everywhere biregular birational transformation of V into a projective space. There is a positive integer m_0 with the following property: let $mX = Y_1, \cdots, Y_t$ be a complete set of representatives of $\mathfrak{N}(mX) \bmod G_a(V)$; then when $m \geqq m_0$, $Y_j - Y_1$, for $j = 1, \cdots, t$, is a complete set of representatives of $G_n(V) \bmod G_a(V)$.*

CHICAGO UNIVERSITY AND
OCHANOMIZU UNIVERISTY, TOKYO.

---

[3] The writer was informed that Mr. Y. Nakai obtained the same result.

REFERENCES.

[1] W. L. Chow, "Abstract theory of the Picard and Albanese varieties," to appear.

[2] ——— and B. L. van der Waerden, "Zur Algebraischen Geometrie IX," *Mathematische Annalen*, vol. 113 (1937), pp. 692-794.

[3] T. Matsusaka, "On the algebraic construction of the Picard variety," *Japanese Journal of Mathematics*, vol. 31 (1951), pp. 217-235.

[4] ———, "On the algebraic construction of the Picard variety II," *ibid.*, vol. 22 (1952), pp. 51-62.

[5] ———, "On the algebraic families of positive divisors," *Journal of the Mathematical Society of Japan*, vol. 5 (1953), pp. 115-136.

[6] ———, "Some theorems on Abelian varieties," *Natural Science Report*, Ochanomizu University, vol. 4 (1953), pp. 164-171.

[7] ———, "On the theorem of Castelnuovo-Enriques," *ibid.*, vol. 4 (1953), pp. 22-35.

[8] A. Néron, "Problèmes arithmétiques et géométriques rattachés à la notion du rang d'une courbe algébriques dans un corps," *Bulletin de la Société Mathématique de France*, vol. 80 (1952), pp. 101-166.

[9] ——— and P. Samuel, "La variété de Picard d'une variété Normale," *Annales de l'institut Fourier*, vol. 4 (1952), pp. 1-30.

[10] G. Shimura, "Reduction of algebraic varieties with respect to a discrete valuation of the basic field," *American Journal of Mathematics*, vol. 77 (1955), pp. 134-176.

[11] B. L. van der Waerden, "Zur Algebraischen Geometrie XIV," *Mathematische Annalen*, vol. 115 (1938), pp. 619-642.

[12] A. Weil, *Foundations of Algebraic Geometry*, American Mathematical Society Colloquium Publications, vol. 29 (1946).

[13] ———, "Variétés Abéliennes et Courbes Algébriques," *Actualités Scientifiques et Industrielles*, No. 1064 (1948).

[14] ———, "Sur les critères d'équivalence en géométrie algébriques," *Mathematische Annalen*, vol. 128 (1954), pp. 95-127.

[15] O. Zariski, "Complete linear systems on normal varieties and a generalization of a lemma of Enriques-Severi," *Annals of Mathematics*, vol. 55 (1952), pp. 552-592.

[16] ———, "Algebraic surfaces," *Ergebnisse der Mathematik und ihrer Grenzgebiete*, vol. 3, no. 5 (1935).

THE NILPOTENCE OF NIL SUBRINGS.*

By M. P. Drazin.

---

1. It is well known that, in any associative ring R with minimal condition on (say) left ideals, every nil left ideal is nilpotent (for the simplest known proof of this, due to R. Brauer, see [4, Theorem 13, p. 64]); more recently, Jacobson has shown ([5], and cf. also [4, Theorem 30, p. 71]) that every nil *subring* of R, besides also certain types of (nil) subsets not admitting the addition and multiplication of R, must be nilpotent. We recall also [4, Theorem 29, p. 71] that, at least in the presence of a two-sided identity element, the minimal condition on left ideals implies the maximal condition on these ideals.

Our main result in this note is that, in any associative ring with maximal condition on nilpotent subrings, every nil subring must in fact be nilpotent. Indeed, we establish the stronger result stated as Theorem 1 below; this may be compared with a result of Levitzki [6], who showed that, if R has maximal condition on both left and right ideals, then every nil subring of R is nilpotent (and that every nil *ideal* is nilpotent under a weaker, though more complicated, hypothesis; cf. also [7]).

In a concluding section, we establish some analogous results for Lie rings.

We note first a trivial lemma, which serves as a starting-point for our arguments in both the succeeding sections:

LEMMA 1. *Let M be any given set, let $s \times t$ be any given binary operation in M, and let A be any subset of M closed under this operation. Then, for any given subsets T of A and U of M, either* (i) $A \leqq U$, *or* (ii) *we can find $a \in A$ and an infinite sequence $t_1, t_2, \cdots$ in T such that* $(\cdots((a \times t_1) \times t_2) \times \cdots) \times t_k \notin U$ $(k = 1, 2, \cdots)$, *or* (iii) *we can find $b \in A$ such that $b \notin U$ and $b \times t \in U$ for all $t \in T$.*

Proof. If (i) is false, then we can certainly choose $a \in A$ with $a \notin U$. Then we have the following inductive method of constructing a sequence $t_1, t_2, \cdots$ satisfying (ii), which method can break down at some stage only if (iii) holds: supposing, for a given positive integer k, that $t_1, \cdots, t_{k-1}$

---

* Received July 30, 1956.

are already defined so that $b=(\cdots(a\times t_1)\times t_2\cdots)\times t_{k-1}\notin U$, then, since $T\leqq A$ and A is closed, we have $b\in A$, and so, if b does not satisfy (iii), we can choose a suitable t_k, and so on.

2. In this section we take M to be an associative ring R (possibly considered as a ring with operators) and, given any subset C of R, we write C^* to denote the subring generated by C. We also now require, for each pair $s,t\in R$, that $s\times t$ should be of the form

$$s\times t=st+xs+y,$$

where both $x=x(s,t)$ and $y=y(s,t)$ are in the subring $\{t\}^*$ of R generated by t; and, when we speak of a *closed* subset A of R, we shall mean that $s\times t\in A$ whenever both $s,t\in A$.

LEMMA 2. *Given any ring R, any closed subset A of R and an arbitrary subset T of A, then either* (1) *$A^*=T^*$, or* (2) *we can find $a\in A$ such that $T^{*i}a+aT^{*i}\neq 0$ $(i=1,2,\cdots)$, or* (3) *we can find $b\in A$ such that $b\notin T^*$ and, for each $t\in T$, $bt\in T^*+T^*b$.*

Proof. We show that, on taking $U=T^*$ in Lemma 1, then (i), (ii), (iii) respectively imply (1), (2), (3). For, if (i) holds, i.e., if $A\leqq T^*$, then of course $A^*\leqq T^*$, while also (since $A\geqq T$) $A^*\geqq T^*$, so (1) follows. Next, for any $t_1,\cdots,t_k\in T$, clearly $(\cdots((a\times t_1)\times t_2)\times\cdots)\times t_k$ is, modulo T^*, a sum of terms of the form $z_1\cdots z_j a z_{j+1}\cdots z_k$ with each $z_i\in T^*$, so that $(\cdots((a\times t_1)\times t_2)\times\cdots)\times t_k\in T^*+\sum_{j=0}^{k}T^{*j}aT^{*k-j}$; if (ii) holds, i.e., if the element on the left is *not* in T^*, then certainly $\sum_{j=0}^{k}T^{*j}aT^{*k-j}\neq 0$ $(k=1,2,\cdots)$, which gives (2) on taking $k=2i-1$. Finally, (iii) gives $b\notin T^*$ and, for any $t\in T$, we have $bt=b\times t-y-xb$, where $b\times t$, $x,y\in T^*$.

Lemmas 1 and 2 are both implicit in Jacobson's paper [5], though he considered only "products" of the more special form $s\times t=st+xs$, with $x=x(s,t)$ an *operator multiple* of t. It is, of course, easy to deduce from (3), as Jacobson did, that $bT^*\leqq T^*+T^*b$; however, Jacobson's own later argument uses only the fact that bT^* is contained in the right ideal of R generated by T, and this is an obvious consequence of (3).

THEOREM 1. *Let R be any given associative ring with maximal condition on nilpotent subrings, and A any closed subset of R. Then, if A is nil (i.e. has all its elements nilpotent), it generates a nilpotent subring of R.*

Proof. We first apply our hypothesis about R to select, from among those subsets B of A which generate nilpotent subrings B^* of R (and certainly such B exist provided that A is not empty), a subset T of A such that T^* is maximal in the class of all subrings B^* arising in this way. Since T^* is nilpotent, it is enough to show that (1) of Lemma 2 holds; and, since the nilpotence of T^* contradicts (2), we need consequently only prove (3) false, i.e., show that no element b of A can have the stated properties.

To do this, let b be as in (3), and let S denote the subring generated by T together with b, so that (since $b \notin T^*$) S contains T^* properly; then, by the maximality of T^* among all the B^*, it will suffice, in order to obtain our desired contradiction, to show that S is itself a B^*, i.e. (since S is certainly generated by a subset of A), that S is nilpotent.

Since A is nil and $b \in A$, we have $b^m = 0$ for some integer $m \geqq 2$. Now, for each positive integer n, every element of S^{mn} is a linear combination of monomials $g = c_1 \cdots c_r$, where $r \geqq mn$ and, for each i, either $c_i = b$ or $c_i \in T$. Also a non-zero g can have no more than $m - 1$ consecutive factors b occurring anywhere in it, so, if q denotes the total number of factors from T occurring, then g can be non-zero only if

$$q \geqq \frac{r-q}{m-1} - 1,$$

so that $q \geqq (r - m + 1)/m \geqq (mn - m + 1)/m$, i.e. $q \geqq n$. In other words, at least n factors from T must occur in any non-zero monomial $g \in S^{mn}$, and so, by use of (3), we can express every element of S^{mn} as a linear combination of products $d_1 \cdots d_q b^j$, where $q \geqq n$, each $d_i \in T^*$ and $0 \leqq j \leqq m - 1$, i.e.

$$S^{mn} \leqq T^{*n} + \sum_{j=1}^{m-1} T^{*n} b^j \qquad (n = 1, 2, \cdots).$$

Hence, since T^* is nilpotent, so is S and the theorem follows.

3. Arguments analogous to most of those in the preceding section can be carried through for Lie rings. This can be done in two ways, by applying Lemma 1 with M taken to be either the given Lie ring itself or the (associative) set of (say) right multiplications of the given ring. However, the results obtainable by the former method seem to be the more interesting, and we shall not discuss the other possible approach further.

From now on, we suppose that we are given a Lie ring L and an operation $s \times t$ in L such that, for each pair $s, t \in L$,

$$s \times t = st + y,$$

where $y = y(s, t)$ is some integral or operator *multiple* of t (and where st is of course now a Lie product). Closure will, naturally, refer to this operation, while C^* will now denote the Lie subring of L generated by a given subset C of L. Corresponding to Lemma 2 above, we now have

LEMMA 3. *Given any Lie ring L, any closed subset A of L and an arbitrary subset T of A, then either* (1′) $A^* = T^*$, *or* (2′) *we can find* $a \in A$ *and an infinite sequence* $t_1, t_2 \cdots$ *in T such that* $(\cdots((at_1)t_2)\cdots)t_k \notin T^*$ $(k = 1, 2, \cdots)$, *or* (3′) *we can find* $b \in A$ *such that* $b \notin T^*$ *and* $bT^* \leqq T^*$.

Proof. We apply Lemma 1 with $U = T^*$, much as before. We deduce (1′) from (i) exactly as in Lemma 2, and this time it is even easier to deduce (2′) from (ii). Finally, (iii) gives $bt \in T^*$ for every $t \in T$, whence the Jacobi identity, together with a straightforward induction on the degrees of the T-monomials involved, gives (3′).

In order to be able to state our next theorem concisely, we introduce some notation and terminology. Given any elements $a_1, a_2, \cdots$ of L, then any product $a_1 a_2 \cdots a_k$ written without parentheses is to be understood as standing for the corresponding left-normed Lie product $(\cdots((a_1a_2)a_3)\cdots)a_k$; and, more generally, given subsets $A_1, A_2, \cdots$ of L, we write $A_1A_2\cdots A_k$ to denote the set of all products of the form $a_1a_2\cdots a_k$ with each $a_i \in A_i$. With these conventions, we can use Bc^k to denote the set of all $(\cdots((zc)c)\cdots)c$ as z runs through B (with just k factors c); similarly, BC^k will denote the set of all $(\cdots((za_1)a_2)\cdots)a_k$ as z runs through B and the a_i run independently through C. We shall call an element c of L *nilpotent on L* if $Lc^k = 0$ for some integer $k = k(c)$, and shall call a subset C of L nilpotent on L if $LC^k = 0$ for some $k = k(C)$; if every element of a subset C of L is nilpotent on L (the implied k's being not necessarily bounded) then we shall call C *nil on L*.

We can now apply Lemma 3, and arguments parallel to those used in proving Theorem 1, to derive

THEOREM 2. *Let L be a given Lie ring with maximal condition on nilpotent subrings (nilpotent being here interpreted in the ordinary Lie sense) and A any closed subset of L. Then, if A is nil on L, the subring of L generated by A is nilpotent on L (and, a fortiori, nilpotent).*

Proof. We first apply the hypothesis on L to select, from among those subsets B of A which generate subrings B^* of L which are nilpotent on L, a subset T of A such that T^* is maximal in the class of all subrings B^* arising in this way. As before, it is enough to show that (1′) of Lemma 3 holds; and, since the nilpotence of T^* on L rules out (2′), we need only prove (3′) false.

Suppose then, by way of contradiction, that A contains an element b satisfying (3′) and let S denote the subring of L generated by T^* together with b, so that S contains T^* properly; then, by the maximality of T^* among the B^*, it is enough to show that S is a B^*, i. e., that S is nilpotent on L.

Since A is nil on L and $b \in A$, we have $Lb^m = 0$ for some $m \geqq 2$, and, since $bT^* = T^*b \leqq T^*$, clearly $S = T^* + Fb$, where F denotes the ring of integers (or any commutative ring of admissible operators). Next, for any $u \in L$, $v \in T^*$, we have, by the Jacobi identity and (3′), that $ubv = uvb + u(bv)$, where $bv \in T^*$, so that

(3″) $ubv - uvb \in uT^*$ *whenever* $u \in L, v \in T^*$.

Now, for any positive integer n, since $S = T^* + Fb$, clearly every element of LS^{mn} is a linear combination of Lie monomials $g = zc_1c_2 \cdots c_{mn}$, where $z \in L$ and, for each i, either $c_i = b$ or $c_i \in T^*$. Also a non-zero g can have no more than $m - 1$ consecutive factors b occurring in it anywhere, so, if q denotes the total number of factors from T^* occurring, then, as before,

$$q \geqq (mn - q)/(m - 1) - 1,$$

i. e., $q \geqq n$. In other words, at least n factors from T^* must occur in any non-zero monomial g, and so, by use of (3″), we can express every element of LS^{mn} as a linear combination of products $zd_1 \cdots d_q b^j$ with $q \geqq n$, each $d_i \in T^*$ and $0 \leqq j \leqq m - 1$, i. e.

$$LS^{mn} \leqq LT^{*n} + \sum_{j=1}^{m-1} LT^{*n}b^j \qquad (n = 1, 2, \cdots).$$

Hence, since T^* is nilpotent on L, so is S and the theorem follows.

Theorem 2 generalizes a result of Zorn [8], who considered only the case in which $s \times t = st$ and $A = L$.

We conclude with two other results, which, though little short of obvious, seem worth putting on record for comparison with Theorem 2 (cf. also [1], [2], [3]):

THEOREM 3. *Let L be a Lie ring with maximal condition on Lie ideals and having characteristic zero. Then, if to each $z \in L$ there corresponds a positive integer $k(z)$ such that $zc^{k(z)} = 0$ for every $c \in L$, we can find a fixed integer k such that $zc^k = 0$ for all $z, c \in L$.*

Proof. For each positive integer j, let X_j denote the set of all $x \in L$

such that $xy^j = 0$ for all $y \in L$. Then it can be shown that each X_j is an ideal of L; we shall not go into the (straightforward but not quite trivial) proof of this fact in detail here, but see e.g. [3, Lemma 4], where a more general result is established. Also clearly $X_j \leqq X_{j+1}$ $(j = 1, 2, \cdots)$, and so, by the maximal condition, there is an integer k such that X_k contains all the other X_j. Thus, for each $z \in L$, we have $z \in X_{k(z)} \leqq X_k$, i.e., $zc^k = 0$ for all $z, c \in L$.

In a precisely similar way, we find

THEOREM 4. *Let L be a Lie ring with maximal condition on Lie ideals and having characteristic zero, and suppose that, to each $z \in L$, there corresponds a positive integer $k(z)$ such that $zL^{k(z)} = 0$. Then L must in fact be nilpotent.*

TRINITY COLLEGE, CAMBRIDGE.

REFERENCES.

[1] M. P. Drazin, "Engel rings and a result of Herstein and Kaplansky," *American Journal of Mathematics*, vol. 77 (1955), pp. 895-913.

[2] K. W. Gruenberg, "Two theorems on Engel groups," *Proceedings of the Cambridge Philosophical Society*, vol. 49 (1953), pp. 377-380.

[3] P. J. Higgins, "Lie rings satisfying the Engel condition," *Proceedings of the Cambridge Philosophical Society*, vol. 50 (1954), pp. 8-15.

[4] N. Jacobson, *The Theory of Rings* (American Mathematical Society, 1943).

[5] ———, "Une généralisation du théorème d'Engel," *Comptes Rendus des Séances de l'Académie des Sciences*, vol. 234 (1952), pp. 579-581.

[6] J. Levitzki, "Solution of a problem of G. Koethe," *American Journal of Mathematics*, vol. 67 (1945), pp. 437-442.

[7] ———, "On multiplicative systems," *Compositio Mathematica*, vol. 8 (1951), pp. 76-80.

[8] M. Zorn, "On a theorem of Engel," *Bulletin of the American Mathematical Society*, vol. 43 (1937), pp. 401-404.

A CHARACTERIZATION OF THE LEBESGUE AREA.*

By Christoph J. Neugebauer.

Introduction. The characterization of the Lebesgue area as a functional Φ defined on a certain class of continuous mappings has attracted a great deal of attention. The conditions that are imposed upon a functional Φ in this paper (see Section 3) are essentially those listed in L. Cesari [2; 7.5]. Let $\mathfrak{T}$ be the class of all continuous mappings (T, A) from an admissible subset A of E_2 into E_3 (see Section 1), and let $L(T, A)$ be the Lebesgue area of (T, A). A subclass $\mathfrak{T}'$ of $\mathfrak{T}$ is considered which consists of all mappings (T, A) in $\mathfrak{T}$ admitting an *elementary shrinking approach* (see Section 4), and it is shown that $\mathfrak{T}'$ is the class of mappings on which each functional Φ satisfying the conditions of Section 3 agrees with the Lebesgue area.

1. Some definitions. We will be concerned with the collection of *admissible* subsets A of the Euclidean plane E_2. By L. Cesari [2; 5.1] this collection comprises (a) all open subsets of E_2, (b) all finite unions of disjoint closed finitely connected Jordan regions, and (c) all open subsets of sets described in (b). The interior of a set A will be denoted by A^0, and the closure of A will be designated by $\bar{A}$. The distance between two point p', p'' of a Euclidean space will be abbreviated by $|p' - p''|$.

Let $\mathfrak{T}$ be the class of all continuous mappings (T, A) from an admissible sets $A \subset E_2$ into the Euclidean three space E_3. The following statements are needed.

(i) A sequence of mappings (T_n, A_n) in $\mathfrak{T}$ is said to *converge* to a mapping (T, A) in $\mathfrak{T}$ provided (1) $A_n \subset A_{n+1} \subset A$, $A_n{}^0 \uparrow A^0$, (2) $d(T, T_n, A_n) \to 0$ as $n \to \infty$, where $d(T, T_n, A_n) = \text{l.u.b.}\, |T(w) - T_n(w)|$, $w \in A_n$ (see [2; 5.3]).

(ii) Let R be the generic notation for the interior of a finite union of disjoint finitely connected Jordan regions. A mapping (T, R) in $\mathfrak{T}$ will be termed *elementary* provided (a) T admits of a continuous extension to $\bar{R}$, (b) there is a quasi-linear mapping Fréchet equivalent to $(T, \bar{R})$. For the concept of Fréchet equivalence see [2; 31.2].

---

* Received March 5, 1956; revised August 17, 1956.

2. Some preliminary results. In this article we will discuss some lemmas which are concerned with Lipschitzian mappings F of constant one from E_3 into E_3. The class of those mappings F will be denoted by $\mathfrak{L}$. The lemma (i) below is a special case of a theorem in E. J. Mickle [5].

(i) LEMMA. *Let B be a subset of E_3 and let F be a Lipschitzian mapping of constant one from B into E_3. Then F can be extended to a Lipschitzian mapping of constant one from E_3 into E_3.*

(ii) LEMMA. *Let (T, A) and (T', A) be two mappings in $\mathfrak{X}$ such that for each w, w' in A, $|T'(w) - T'(w')| \leqq |T(w) - T(w')|$. Then there exists a mapping F in $\mathfrak{L}$ such that $(T', A) = (FT, A)$.*

Proof. Let γ be a set in A on which T is constant. Then by hypothesis T' is also constant on γ. Therefore, the mapping $F' = T'T^{-1}$ is a single-valued transformation from $T(A)$ onto $T'(A)$. We assert next that $|F'(p) - F'(p')| \leqq |p - p'|$, $p, p' \in T(A)$. For $p, p' \in T(A)$ let w, w' be two points in A for which $T(w) = p$, $T(w') = p'$. Then

$$|F'(p) - F'(p')| = |T'T^{-1}(p) - T'T^{-1}(p')|$$
$$= |T'(w) - T'(w')| \leqq |T(w) - T(w')| = |p - p'|.$$

By (i), F' admits an extension F to E_3 satisfying the desired properties.

(iii) LEMMA. *Let (T_0, A_0) be a fixed mapping in $\mathfrak{X}$ and let (T_n, A_n), $n = 1, 2, \cdots$, be a sequence of mappings in $\mathfrak{X}$ satisfying* (1) *$(T_n, A_n) \to (T, A)$, $(T, A) \in \mathfrak{X}$, $A \subset A_0$,* (2) *for each n, there is a mapping $F_n \in \mathfrak{L}$ such that $(T_n, A_n) = (F_n T_0, A_n)$. Then there exists a mapping $F \in \mathfrak{L}$ with the property that $(T, A) = (FT_0, A)$.*

Proof. Let w, w' be any two points in A and let $\{w_i\}$, $\{w_i'\}$ be two sequences in A^0 such that $w_i \to w$, $w_i' \to w'$. Since by 1(i), $A_n \subset A_{n+1} \subset A$, $A^0{}_n \uparrow A^0$, we may choose integers $n_1 < n_2 < \cdots < n_i < \cdots$ such that w_i, w_i' are both in $A^0{}_{n_i}$. Now, since $T(w_i) \to T(w)$, $T(w_i') \to T(w')$, and since in view of 1(i), $|T(w_i) - T_{n_i}(w_i)| \to 0$, $|T(w_i') - T_{n_i}(w_i')| \to 0$ as $i \to \infty$, we conclude that $T_{n_i}(w_i) \to T(w)$, $T_{n_i}(w_i') \to T(w')$. Moreover, the continuity of T_0 implies $T_0(w_i) \to T_0(w)$, $T_0(w_i') \to T_0(w')$.

Let $\epsilon > 0$ be given. Then we can determine an integer $J > 0$ such that for $i > J$,

$$|T(w) - T_{n_i}(w_i)| < \epsilon/3, \qquad |T(w') - T_{n_i}(w_i')| < \epsilon/3,$$
$$|T_0(w_i) - T_0(w_i')| < |T_0(w') - T_0(w)| + \epsilon/3.$$

Since $T_{n_i}(w_i) = F_{n_i}T_0(w_i)$, $T_{n_i}(w_i') = F_{n_i}T_0(w_i')$, there follows for $i > J$,

$$\begin{aligned} |T(w) - T(w')| &\leqq |T(w) - T_{n_i}(w_i)| + |T_{n_i}(w_i) - T_{n_i}(w_i')| \\ &+ |T_{n_i}(w_i') - T(w')| \leqq |T(w) - T_{n_i}(w_i)| + |T_0(w_i) - T_0(w_i')| \\ &+ |T_{n_i}(w_i') - T(w')| < |T_0(w) - T_0(w')| + \epsilon. \end{aligned}$$

Since $\epsilon > 0$ was arbitrary, $|T(w) - T(w')| \leqq |T_0(w) - T_0(w')|$. By (ii) the proof is complete.

3. Class $\mathfrak{T}^*$. Let $\mathfrak{F}$ be the class of all functionals $\Phi(T, A)$ defined for $(T, A) \in \mathfrak{T}$ satisfying the following conditions:

(a) $\Phi(T, A) \geqq 0$ for $(T, A) \in \mathfrak{T}$.

(b) $\Phi(T, A)$ is lower semi-continuous, i.e., if $(T_n, A_n) \rightarrow (T, A)$, then $\Phi(T, A) \leqq \liminf_{n \to \infty} \Phi(T_n, A_n)$.

(c) $\Phi(T, A)$ satisfies the Kolmogoroff principle, i.e., for $F \in \mathfrak{L}$, $\Phi(FT, A) \leqq \Phi(T, A)$.

(d) $\Phi(T, A)$ is monotone, i.e., for $(T, A) \in \mathfrak{T}$ and A' an admissible subset of A, $\Phi(T, A') \leqq \Phi(T, A)$.

(e) For (T, R) an elementary mapping (see Section 1(ii)), $\Phi(T, R) = L(T, R)$.

Remark. The Lebesgue area $L(T, A)$ satisfies the above conditions and hence is a functional in $\mathfrak{F}$ (see [2]). For each $\Phi \in \mathfrak{F}$ and each $(T, A) \in \mathfrak{T}$ we have $\Phi(T, A) \leqq L(T, A)$ (see [2; 5.12]).

For every $\Phi \in \mathfrak{F}$ let $\mathfrak{T}(\Phi)$ be the class of mappings $(T, A) \in \mathfrak{T}$ for which $\Phi(T, A) = L(T, A)$. Finally, let $\mathfrak{T}^* = \cap\, \mathfrak{T}(\Phi)$, $\Phi \in \mathfrak{F}$. In view of (e), $\mathfrak{T}^*$ contains all elementary mappings.

4. Class $\mathfrak{T}'$. *Definition.* A mapping $(T, A) \in \mathfrak{T}$ is said to satisfy the *condition* (s) provided for every $\epsilon > 0$ there exists an elementary mapping (T', R) (see Section 1(ii)) with $R \subset A$ and

$$(1) \qquad |T'(w) - T'(w')| \leqq |T(w) - T(w')|, \qquad w, w' \in R$$

$$(2) \qquad L(T, A) - L(T', R) < \epsilon, \text{ if } L(T, A) < \infty, \; L(T', R) > \epsilon^{-1} \text{ if } L(T, A) = +\infty.$$

It may be of interest to note that (1) does not imply that (T', R) approximates (T, A). It is only required that $L(T', R)$ approximates $L(T, A)$.

Let us denote by $\mathfrak{T}'$ the class of all mappings (T,A) in $\mathfrak{T}$ which satisfy the condition (s). Concerning the class $\mathfrak{T}'$ we have the following two lemmas.

(i) Lemma. *The class $\mathfrak{T}'$ contains all elementary mappings as well as all mappings (T,A) for which $L(T,A)=0$.*

Proof. The first statement is obvious, and for the second it suffices to let (T',R), $R\subset A$, be constant on R.

(ii) Lemma. *If (T,A) is in $\mathfrak{T}'$, then (T,A^0) is also in $\mathfrak{T}'$.*

Proof. Since (T,A) is in $\mathfrak{T}'$ there is, for $\epsilon>0$ given, an elementary mapping (T',R), $R\subset A$, such that (1) and (2) are satisfied. Since (T',R) is elementary, the set R is an open subset of E_2 (see Section 1(ii)). Hence $R\subset A^0$, and since $L(T,A)=L(T,A^0)$, the mapping (T,A^0) is in $\mathfrak{T}'$.

5. Main result. We are now ready to prove

Theorem. $\mathfrak{T}^*=\mathfrak{T}'$.

Proof. In view of Section 3 we have for every $\Phi\in\mathfrak{F}$ and for every $(T,A)\in\mathfrak{T}$ the inequality $\Phi(T,A)\leqq L(T,A)$. We will first prove that $\mathfrak{T}^*\supset\mathfrak{T}'$. If we deny this inclusion, we have a functional $\Phi\in\mathfrak{F}$ and a mapping (T,A) in $\mathfrak{T}'$ such that $\Phi(T,A)<L(T,A)$. Since (T,A) satisfies the condition (s), there is an elementary mapping (T',R), $R\subset A$, such that $L(T',R)>\Phi(T,A)$ and

$$(1)\qquad |T'(w)-T'(w')|\leqq|T(w)-T(w')|,\qquad w,w'\in R.$$

In view of the conditions 3(d), (e), we infer that

$$(2)\qquad \Phi(T',R)=L(T',R)>\Phi(T,A)\geqq\Phi(T,R).$$

However, from 2(ii) and 3(c) we deduce by (1) $\Phi(T',R)\leqq\Phi(T,R)$, a contradiction with (2). Therefore, $\mathfrak{T}^*\supset\mathfrak{T}'$.

6. To prove the complementary inclusion $\mathfrak{T}^*\subset\mathfrak{T}'$, let us assume that there is a mapping (T_0,A_0) in $\mathfrak{T}^*$ which is not in $\mathfrak{T}'$. From 4(i) we have that $L(T_0,A_0)>0$. There exists now a number $\lambda_0\geqq 0$ with $L(T_0,A_0)>\lambda_0$ such that for every elementary mapping (T',R), $R\subset A_0$, for which $|T'(w)-T'(w')|\leqq|T_0(w)-T_0(w')|$, $w,w'\in R$, we have $L(T',R)\leqq\lambda_0$.

Let $\mathfrak{K}_0$ be the class of mappings (T,A') in $\mathfrak{T}$ such that (1) $A'\subset A_0$, (2) there exists a mapping $F\in\mathfrak{L}$ such that $(T,A')=(FT_0,A')$, (3) $L(T,A')>\lambda_0$. Finally, let $\mathfrak{K}_0'$ be the class of mappings $(T,A)\in\mathfrak{T}$ for which there exists a sequence $(T_n, A_n) \in \mathfrak{R}_0$ such that $(T_n, A_n) \to (T, A)$ and $L(T, A) > \lambda_0$. Note that $\mathfrak{R}_0 \subset \mathfrak{R}_0'$, and if A_0 is compact then $\mathfrak{R}_0 = \mathfrak{R}_0'$.

7. In this paragraph we will prove some lemmas concerning the class $\mathfrak{R}_0'$.

(i) LEMMA. *If* $(T, A) \in \mathfrak{R}_0'$, *then* $(T, A^0) \in \mathfrak{R}_0$.

Proof. We have a sequence of mappings $(T_n, A_n) \in \mathfrak{R}_0$ such that $(T_n, A_n) \to (T, A)$ and $L(T, A) > \lambda_0$. By 1(i), $A_n \subset A_{n+1} \subset A$, $A_n^0 \uparrow A^0$. Since also $A_n \subset A_0$, $n = 1, 2, \cdots$, the set A^0 is a subset of A_0. For each n, there is a mapping $F_n \in \mathfrak{L}$ for which $(T_n, A_n^0) = (F_n T_0, A_n^0)$. Since clearly $(T_n, A_n^0) \to (T, A^0)$, we have by 2(iii) a mapping $F \in \mathfrak{L}$ such that $(T, A^0) = (F T_0, A^0)$. Since, finally, $L(T, A^0) = L(T, A) > \lambda_0$, we infer from the definition of $\mathfrak{R}_0$ that $(T, A^0) \in \mathfrak{R}_0$.

(ii) LEMMA. $\mathfrak{R}_0'$ *contains no elementary mappings.*

Proof. If (T, R) is an elementary mapping in $\mathfrak{R}_0'$, then from 1(ii), $R = R^0$. Thus by (i), $(T, R) \in \mathfrak{R}_0$. But then from the definition of $\mathfrak{R}_0$ we have a mapping $F \in \mathfrak{L}$ such that $(T, R) = (F T_0, R)$ and $L(T, R) > \lambda_0$. In view of Section 6 this is impossible and hence $\mathfrak{R}_0'$ contains no elementary mappings.

(iii) LEMMA. *Let* (T, A) *be in* $\mathfrak{R}_0'$ *and let* A' *be an admissible subset of* A. *Assume there is a mapping* $F \in \mathfrak{L}$ *such that* $L(FT, A') > \lambda_0$. *Then* $(FT, A') \in \mathfrak{R}_0'$.

Proof. We have a sequence (T_n, A_n) in $\mathfrak{R}_0$ such that $(T_n, A_n) \to (T, A)$. Since the sets $A_n' = A_n \cap A'$ satisfy the properties $A_n' \subset A_{n+1}' \subset A'$, $A_n'^0 \uparrow A'^0$, we have that $(FT_n, A_n'^0) \to (FT, A')$. From $L(FT, A') > \lambda_0$, we have as a consequence of the lower semi-continuity of the Lebesgue area, $L(FT_n, A_n'^0) > \lambda_0$ for n large. Thus $(FT_n, A_n'^0)$ is in $\mathfrak{R}_0$ for n large, and the lemma follows.

(iv) LEMMA. *Let* (T_n, A_n) *be a sequence in* $\mathfrak{R}_0'$ *such that* $(T_n, A_n) \to (T, A)$. *Then, if* $L(T, A) > \lambda_0$, *the mapping* (T, A) *is in* $\mathfrak{R}_0'$.

Proof. From (i), (T_n, A_n^0) is in $\mathfrak{R}_0$ for each n, and from 1(i), $(T_n, A_n^0) \to (T, A)$. Thus, (T, A) is in $\mathfrak{R}_0'$.

8. Define a functional $\Phi(T, A)$ for $(T, A) \in \mathfrak{T}$ as follows: $\Phi(T, A) = \lambda_0$ if $(T, A) \in \mathfrak{R}_0'$, and $\Phi(T, A) = L(T, A)$ otherwise. We will verify now that

$\Phi(T,A)$ satisfies the conditions of Section 3. Since 3(a) is obvious, we will prove that

(b) $\Phi(T,A)$ is lower semi-continuous.

Proof. Let (T_n, A_n) be a sequence of mappings in $\mathfrak{T}$ which converges to (T,A). Then $L(T,A) \leqq \liminf L(T_n, A_n)$ as $n \to \infty$. Hence, if $L(T,A) \leqq \lambda_0$, then $\Phi(T,A) \leqq \liminf \Phi(T_n, A_n)$, from the definition of $\Phi(T,A)$. Assume now that $L(T,A) > \lambda_0$. Then there exists an integer $N > 0$ such that for $n > N$, $L(T_n, A_n) > \lambda_0$. Hence for $n > N$, $\lambda_0 \leqq \Phi(T_n, A_n) \leqq L(T_n, A_n)$. If $(T,A) \in \mathfrak{K}_0'$, we infer that $\Phi(T,A) \leqq \liminf \Phi(T_n, A_n)$. If (T,A) is not in $\mathfrak{K}_0'$, then by 7(iv), only a finite number of the (T_n, A_n) can be in $\mathfrak{K}_0'$. Thus $\Phi(T,A) \leqq \liminf \Phi(T_n, A_n)$.

(c) $\Phi(T,A)$ satisfies the Kolmogoroff principle.

Proof. Let F be in $\mathfrak{L}$. If (T,A) is not in $\mathfrak{K}_0'$, then clearly $\Phi(FT,A) \leqq L(FT,A) \leqq L(T,A) = \Phi(T,A)$. Assume now that (T,A) is in $\mathfrak{K}_0'$. If $L(FT,A) > \lambda_0$, we conclude from 7(iii) that (FT,A) is in $\mathfrak{K}_0'$, and hence $\Phi(FT,A) = \Phi(T,A)$. If $L(FT,A) \leqq \lambda_0$, then clearly $\Phi(FT,A) = L(FT,A) \leqq \lambda_0 = \Phi(T,A)$.

(d) $\Phi(T,A)$ is monotone.

Proof. This is a ready consequence of the definition of Φ and $\mathfrak{K}_0'$.

(e) $\Phi(T,R) = L(T,R)$ if (T,R) is elementary.

Proof. If (T,R) is elementary, then it follows from 7(ii) that (T,R) is not in $\mathfrak{K}_0'$. Therefore, (e) is a consequence of the definition of Φ.

Under the assumption that there is a mapping (T_0, A_0) in $\mathfrak{T}^*$ not in $\mathfrak{T}'$ there can be exhibited a functional $\Phi \in \mathfrak{F}$ such that $\Phi(T_0, A_0) < L(T_0, A_0)$. But this contradicts the definition of $\mathfrak{T}^*$, and therefore $\mathfrak{T}^* \subset \mathfrak{T}'$. With the inclusion established in Section 5, the proof of the main result is complete.

9. Lemma. *For* $\Phi \in \mathfrak{F}$ *and* $(T,A) \in \mathfrak{T}^*$ *we have* $\Phi(T,A^0) = \Phi(T,A)$.

Proof. From 5, (T,A) is in $\mathfrak{T}'$ and from 4(ii), (T,A^0) is in $\mathfrak{T}'$. Thus $\Phi(T,A^0) = L(T,A^0) = L(T,A) = \Phi(T,A)$.

10. A definite relation between the classes $\mathfrak{T}'$ and $\mathfrak{T}$ is not known to the writer. A solution of this problem would answer the question whether or not the conditions listed in Section 3 suffice to characterize the Lebesgue area. In this connection the following comments are in order. The condition 3(e) is concerned with Fréchet equivalence. If one were to modify the condition 3(e) to (e′) by replacing Fréchet equivalence by Lebesgue equivalence in 3(e), then an example of a functional satisfying the conditions 3(a), (b), (c), (d) and (e′) can be exhibited which does not agree with the Lebesgue area. An example of such a functional will be pubilshed elsewhere.

PURDUE UNIVERSITY.

REFERENCES.

[1] J. Cecconi, "Sull' area di Peano e sulla definizione assiomatica dell' area di una superficie," *Rendiconti del Seminario Matematico della Univeristà di Padova,* vol. 20 (1951), pp. 307-314.

[2] L. Cesari, *Surface Area,* Princeton University Press, 1956.

[3] ———, "L'area di Lebesgue come una misura," *Rendiconti di Matematica e delle sue Applicazioni,* Roma, (5) 14, 1955, pp. 655-673.

[4] G. Scorza Dragoni, "Sulla definizione assiomatica dell' area di una superficie," *Rendiconti del Seminario Matematico della Università di Padova,* vol. 5 (1946), pp. 8-24.

[5] E. J. Mickle, "On the extension of a transformation," *Bulletin of the American Mathematical Society,* vol. 55 (1949), pp. 160-164.

[6] M. Pagni, "Sulla definizione dell' area di una superficie per via assiomatica," *Rendiconti del Seminario Matematico della Università di Padova,* vol. 19 (1950), pp. 303-316.

[7] T. Radó, *Length and Area,* American Mathematical Society Colloquium Publications, vol. 30 (1948).

[8] E. Silverman, "Definition of Lebesgue area for surfaces in metric spaces," *Rivista di Matematica della Università di Parma,* vol. 2 (1951), pp. 47-76.

[9] G. Stampacchia, "Sulla definizuone assiomatica dell' area di una superficie rettificabile," *Rendiconti Accademia Nazionale di Lincei,* vol. 2 (1947), pp. 542-546.

[10] G. Zwirner, "Sulla definizione d'area di una superficie," *Istituto Veneto di Scienze, Lettere ed Arti Venezia,* vol 97, 2 (1937-38), pp. 409-416.

WEAKLY STANDARD RINGS.*

By R. L. San Soucie.

1. Introduction.

1. Introduction. Generalizing the standard algebras of Albert (see [1], p. 576), Kleinfeld [5] has called a ring *accessible* if the following identities hold:

$$(x,y,z)+(z,x,y)-(x,z,y)=0, \tag{1.1}$$

$$((w,x),y,z)=0, \tag{1.2}$$

where the associator (x,y,z) and the commutator (w,x) are defined by

$$(x,y,z)=xy\cdot z-x\cdot yz, \qquad (w,x)=wx-xw. \tag{1.3}$$

The substitution of x for z in (1.1) gives the relation

$$(x,y,x)=0, \tag{1.4}$$

so that accessible rings are *flexible* (see [1], p. 561). A linearization of the flexible law yields the identity

$$(x,y,z)=-(z,y,x), \tag{1.5}$$

valid in any flexible ring. Hence it follows from (1.2), (1.5) and (1.1) that the following identity also holds in an accessible ring:

$$(w,(x,y),z)=0. \tag{1.6}$$

We propose, therefore, to call a ring, R, *weakly standard*[1] if R is flexible and if identities (1.2) and (1.6) hold in R. Thus the accessible rings of Kleinfeld, as well as the standard algebras of Albert, are automatically

---

* Received July 10, 1956.

[1] Kleinfeld's analogue of our Theorem 2 was announced by him in an abstract which appeared in the January 1956 *Bulletin* and it was this result of his, as published, which called our attention to these matters. We then generalized the concept of accessible ring to that of weakly standard ring, and proved Theorems 1, 2, and 3, as well as a weaker version of Theorem 4, requiring also the absence of non-zero nilpotent elements. Subsequent communication with Kleinfeld informed us that his results, for accessible rings, also included the prime, primitive and semi-simple cases, although not included in his abstract. Hence our work on Theorems 1 and 3 was independent. The author hereby acknowledges this communication with Kleinfeld and notes, with thanks, that Kleinfeld provided him with a copy of his manuscript of [5], prior to its publication.

weakly standard. On the other hand, we shall give an example later in the paper of a weakly standard ring which is not accessible.

The results obtained parallel those of Kleinfeld for accessible rings, but the method is different. We first show that a prime ring is weakly standard if and only if it is either associative or commutative, and then we prove that simple rings and primitive rings are prime, with the exception of rings R such that $R^2 = 0$. But for these the conclusion holds trivially. The Brown-Jacobson theory for arbitrary rings then yields a structure theorem for semi-simple weakly standard rings.

Section 3 of the paper is concerned with a proof of the fact that simple flexible rings satisfying (1.2) are either associative or commutative. This generalizes the result for weakly standard rings but appears to be of considerable interest in itself. Various applications of this theorem are mentioned.

The last section contains the example referred to above, as well as examples showing the impossibility of making certain plausible generalizations in our hypotheses.

Throughout the paper we use the letters t, u, v, w, x, y, z to stand for arbitrary elements of the ring under consideration, thus obviating expressions like "for all x and y of the ring."

2. Main results. To facilitate our computations, we begin by defining the following functions:

$$f(w,x,y,z) = (wx,y,z) - (w,xy,z) + (w,x,yz) - w(x,y,z) - (w,x,y)z, \tag{2.1}$$

$$g(x,y,z) = (xy,z) - x(y,z) - (x,z)y - (x,y,z) - (z,x,y) + (x,z,y). \tag{2.2}$$

It is well known that each of these functions is identically zero in any ring whatever. We now assume that R is a flexible ring and make

Definition 1. Let

$$S = [s \in R \mid (s,x,y) = 0], \qquad M = [m \in R \mid (x,m,y) = 0].$$

Then we call S the *left nucleus* of R and M the *center nucleus.*

With these definitions, the flexible ring R is weakly standard if and only if commutators are in $S \cap M$. For any $s \in S$, $f(s,x,y,z) = 0$ implies that $(sx,y,z) = s(x,y,z)$ while (1.5) implies that $(x,y,s) = 0$.

Definition 2. A ring R is called *prime* if, whenever I and J are ideals of R such that $IJ = 0$, then either $I = 0$ or $J = 0$.

Our first goal is to prove that a prime ring is weakly standard if and only if it is either associative or commutative. We take a significant step in this direction by letting C be the set of all commutators of a weakly standard ring R and proving

Lemma 1. *If A is the set of all finite sums of elements of the form $R(C,R)$, then A is an ideal of R.*

Proof. That A is a left ideal is immediately obvious in view of the definition of a weakly standard ring. For any commutator $c \in C$, $g(u,v,c) = 0$ implies that

$$(c,uv) = u(c,v) + (c,u)v. \tag{2.3}$$

Hence consider $x((y,z),u) \cdot v$ and let $c = (y,z)$. Then we get

$$x(c,u) \cdot v = x \cdot (c,u)v = x(c,uv) + xu \cdot (c,v).$$

Thus A is also a right ideal and the lemma is proved.

Corollary. *The set B of all finite sums of elements of the form $(C,R)R$ is an ideal of R.*

Henceforth we assume that R is a not associative, weakly standard, prime ring. It follows immediately that R does not have any non-zero absolute zero divisors, since the set of all such absolute zero divisors forms an ideal Z such that $RZ = 0$.

Lemma 2. $(C,R) = 0$.

Proof. Assume that there exist elements d, e, f in R such that $((d,e),f) \neq 0$ and let $Q = [q \in R \mid q(C,R) = (C,R)q = 0]$. It is easy to verify, using (2.3), that Q is an ideal of R. To prove that $Q \neq 0$ we suppose the contrary and let $c = (x,y)$. From $g(z,c,w) = 0$ we get that $(zc,w) = z(c,w) + (z,w)c$ so that $z(c,w)$ is an element of S. Consequently $(c,w)(z,t,v) = 0$ and also $(z,t,v)(c,w) = 0$. But this implies that all associators are in Q, R is associative, and this is a contradiction. We must therefore conclude that $Q \neq 0$. However, $AQ = QB = 0$ implies that $A = B = 0$, and from this we are led to the fact that $((d,e),f)$ is an absolute zero divisor and hence zero. The now inescapable conclusion is that the lemma is proved.

Henceforth assume that R is not commutative either and select a, b in R such that $d = (a,b) \neq 0$. Let $P = [p \in R \mid pd = dp = 0]$, and observe that P is an ideal of R. Assume for the moment that $P = 0$. From $g(a,b,b) = 0$ we infer that $(ab,b) = db$. Thus $0 = ((ab,b),a) = -d^2$ and this implies that $d = 0$, a contradiction. Therefore $P \neq 0$. However, Rd is an ideal of R and $RdP = 0$. The hypothesis on R forces the conclusion that $Rd = 0$, from which d is an absolute zero divisor and hence zero. This contradiction shows that R must, in fact, be commutative. We have all but proved

THEOREM 1. *Let R be a prime ring. Then R is weakly standard if and only if R is either commutative or associative.*

Proof. It remains only to remark that a commutative ring is flexible with $(R,R) = 0$, while an associative ring is automatically weakly standard.

We are now in a position to derive a structure theory for weakly standard rings. If R is simple[2] and $R^2 = 0$, R is both associative and commutative. If R is simple and $R^2 \neq 0$, then R is prime. We consequently have

THEOREM 2. *Let R be a simple ring. Then R is weakly standard if and only if R is either associative or commutative.*

Let us now recall that a ring R is called *primitive* if R contains a regular maximal right ideal E which contains no two-sided ideal of R other than the zero ideal. The following lemma was proved by Kleinfeld [5] using the hypothesis of accessibility. We do not use the hypothesis.

LEMMA 3. *Let R be an arbitrary primitive ring. Then R is a prime ring.*

Proof. Suppose E is a maximal right ideal of R such that $ex - x$ is in E for all x in R and for some e in R. Let I and J be two ideals of R such that $IJ = 0$ and assume that $I \neq 0$. Then $I \not\subset E$ so $R = E + I$ and $RJ = EJ \subset E$. Hence $ej \in E$ and thus $-j \in E$, $J \subset E$ and $J = 0$.

As an immediate application of the lemma we have

THEOREM 3. *Let R be a primitive ring. Then R is weakly standard if and only if R is either associative or commutative.*

Since it follows from a theorem of Brown (see [4], p. 116) that a semi-simple ring is a subdirect sum of primitive rings, the structure theory for semi-simple weakly standard rings is completely determined by Theorem 3.

---

[2] By a simple ring we mean one which has no proper two-sided ideals.

3. Simple flexible rings. In this section we show that it is possible to improve upon Theorem 2, but in a way that does not seem, at this writing, to carry over to the results of Theorems 1 or 3. The starting point is a remark by Kleinfeld in [5] to the effect that, if D is the set of all finite sums of elements of the form (R,R,R) and $R(R,R,R)$, then D is an ideal of R, where R is any ring whatever.

Assume now that R is flexible and that $(R,R) \subset S$. From $g(x,y,y)=0$ we get $(xy,y)=(x,y)y$ and this identity implies

$$(x,y)(y,u,v)=0. \tag{3.1}$$

A linearization of (3.1) yields $(x,z)(y,u,v)+(x,y)(z,u,v)=0$ and the substitution $z=s$ gives

$$(x,s)(y,u,v)=0. \tag{3.2}$$

A similar argument, together with (1.5), implies the analogous

$$(y,u,v)(x,s)=0. \tag{3.3}$$

At this point we add the requirement that R be a simple ring. If the ideal $D=0$, then R is associative. If $D\neq 0$, the simplicity of R requires that $D=R$. Consequently, any t in R can be expressed as a finite sum of elements of the form (R,R,R) and $R(R,R,R)$. Thus, for any (x,s), (3.3) implies that $t(x,s)=0$. A similar argument, using elements of the form (R,R,R) and $(R,R,R)R$, as well as (3.2), gives $(x,s)t=0$, and therefore (x,s) is an absolute zero divisor. We now have two alternatives: if some $(x,s)\neq 0$, the ideal of absolute zero divisors is all of R and R is both associative and commutative; on the other hand, if $(x,s)=0$, then commutators are automatically in M and Theorem 2 applies. We have proved

THEOREM 4. *Let R be a simple flexible ring. Then commutators are in the left nucleus of R if and only if R is either commutative or associative.*

This result is a considerable generalization of Albert's Theorem 14 ([1], p. 593) that a simple standard algebra is either an associative or a Jordan algebra. But the theorem has other applications. Albert has also proved ([2], p. 519) that a simple, commutative, power-associative algebra, of characteristic prime to 30 and of degree greater than two, is a Jordan algebra. Our Theorem 4 shows that the conclusion of Albert's theorem holds with less restrictive hypotheses. The same remarks apply to Albert's Theorems 1 and 2 in [3].

4. Examples.

Example 1. Let A be an alternative ring of characteristic prime to 3 generated by three elements x, y, z such that $(x,y,z) \neq 0$. Let B be the alternative ring obtained from A by setting all products (in A) containing at least four factors equal to zero, and by preserving all other sums and products. Then $(x,y,z) \neq 0$ in B also. Moreover, B is flexible and trivially weakly standard. However, B does not satisfy (1.1), for otherwise $(x,y,z) = 0$ as a consequence of the alternative law.

This gives an example of a weakly standard ring that is not accessible. Thus our results generalize and subsume those of Kleinfeld in [5].

Example 2. In [1], pp. 588-589, Albert gives an example of a simple flexible algebra over any field F of characteristic not two. A not difficult calculation shows that commutators are not in the left nucleus. This example proves that the hypothesis of Theorem 4 could not be "simple flexible" instead of "simple flexible with commutators in the left nucleus."

Example 3. Let A be an algebra over a field F with basis elements e, u, v, w, z, where the only non-zero products among the basis elements are $e^2 = e$, $eu = ue = v$, $ev = ve = u$, $we = ze = w$. If

$$x = \alpha_1 e + \alpha_2 u + \alpha_3 v + \alpha_4 w + \alpha_5 z,\ y = \beta_1 e + \beta_2 u + \beta_3 v + \beta_4 w + \beta_5 z,$$
$$\text{and } t = \gamma_1 e + \gamma_2 u + \gamma_3 v + \gamma_4 w + \gamma_5 z$$

are arbitrary elements of A (with the α_i, β_i and γ_i in F), a straightforward calculation shows that

$$(4.1) \quad (x,y,t) = (\alpha_2\beta_1\gamma_1 + \alpha_1\beta_1\gamma_3 - \alpha_3\beta_1\gamma_1 - \alpha_1\beta_1\gamma_2)u$$
$$+ (\alpha_3\beta_1\gamma_1 + \alpha_1\beta_1\gamma_2 - \alpha_2\beta_1\gamma_1 - \alpha_1\beta_1\gamma_3)v.$$

It is easy to see from (4.1) that $(x,y,x) = 0$ so that A is a flexible algebra. Moreover, $\beta_1 = 0$ makes the right hand side of (4.1) vanish. It therefore follows that

$$(4.2) \qquad M = [m \in A \mid m = m_2 u + m_3 v + m_4 w + m_5 z].$$

Direct computation shows that

$$(4.3) \qquad S = [s \in A \mid s = s_2 u + s_2 v + s_3 w + s_4 z].$$

Now (4.2) and (4.3) together imply that $S \subset M$. Finally

$$(4.4) \qquad (x,y) = (\alpha_4\beta_1 + \alpha_5\beta_1 - \alpha_1\beta_4 - x_1\beta_5)w$$

and from this we conclude that commutators are in $S \cap M$. However A is neither associative nor commutative, so that the weakly standard hypothesis alone is not enough for Theorem 2.

Example 4.[3] Let A be an algebra over any field F of characteristic not two and with basis elements e, u, v, where the only non-zero products among basis elements are $e^2 = e$, $eu = ve = v$, $ue = u - v$. Calculations as outlined above show that A is flexible, that $S \subset M$, that commutators are in M, but that commutators are not in S. Hence the definition of weakly standard ring cannot be modified in this direction.

Example 5. Let A be an algebra as above with basis e, u, v, w, where $e^2 = e$, $eu = ue = vw = u$, $wv = -u$, and all other basis products zero. It is easy to see that A is not flexible, but that commutators associate in any of the three places in the associator. Thus the definition of weakly standard ring cannot be modified in this direction either.

THE UNIVERSITY OF OREGON.

REFERENCES.

[1] A. A. Albert, "Power-associative rings," *Transactions of the American Mathematical Society*, vol. 64 (1948), pp. 552-593.

[2] ———, "A theory of power-associative commutative algebras," *ibid.*, vol. 69 (1950), pp. 503-527.

[3] ———, "On commutative power-associative algebras of degree two," *ibid.*, vol. 74 (1953), pp. 323-343.

[4] B. Brown, "An extension of the Jacobson radical," *Proceedings of the American Mathematical Society*, vol. 2 (1951), pp. 114-117.

[5] E. Kleinfeld, "Standard and accessible rings," *Canadian Journal of Mathematics*, vol. 8 (1956), pp. 335-340.

---

[3] Examples 4 and 5 were constructed by Albert in [1] for a different purpose than we use them here.

DIFFERENTIAL OPERATORS ON A SEMISIMPLE LIE ALGEBRA.*

By Harish-Chandra.

1. Introduction. The object of this paper is to present in as concise and coherent a form as possible, certain results on differential operators which will be needed in two subsequent papers for application to the theory of Fourier transforms on a semisimple Lie algebra $\mathfrak{g}_0$. When $\mathfrak{g}_0$ is compact, this theory is not difficult (see Section 5) although some of the results obtained here (e. g. Thsorems 2 and 3) seem to be new. Therefore the main application of our results will be to the case when $\mathfrak{g}_0$ is noncompact. There it will appear that one can obtain certain formulas of a more or less analytic (as against algebraic) nature, which bear a great resemblance to their counterparts in the compact case (see [4(i)]). However, in view of their non-algebraic character, it would seem rather unlikely that the main burden of their proof could be transferred to the compact case by some formal device such as the "unitarian trick." For instance, let us consider the following example. Let $\mathfrak{g}$ the the Lie algebra of all 2×2 complex matrices of trace zero and G_c its (connected) complex adjoint group. Let $\mathfrak{g}_0$ and $\mathfrak{u}$ be the real subalgebras of $\mathfrak{g}$ consisting of the real and the skew-hermitian matrices respectively and G, U the corresponding real analytic subgroups of G_c. Then $\mathfrak{g}_0 \cap \mathfrak{u} = \mathfrak{h}_0$, where $\mathfrak{h}_0$ is the vector space spanned over the real field R by $H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Let f, g be functions of class C^∞ on $\mathfrak{g}_0$ and $\mathfrak{u}$ respectively which vanish outside a compact set. Put

$$\phi_f(t) = t \int_G f(txH)\,dx, \qquad \psi_g(t) = t \int_U g(tuH)\,du \qquad\qquad (t \in R)$$

where dx and du are the Haar measures on G and U respectively. It is not difficult to show that ϕ_f is well defined and of class C^∞ for all $t \neq 0$ and one can prove that

$$\operatorname*{Lim}_{t\to 0}((d/dt)\phi_f) = c_1 f(0), \qquad \operatorname*{Lim}_{t\to 0}((d/dt)\psi_g(= c_2 g(0)$$

where c_1, c_2 are nonzero constants independent of f and g. The proof of this formula is quite trivial for g and follows from the fact that

$$\operatorname*{Lim}_{t\to 0} \int_U g(tuH)\,du = g(0),$$

---

* Received July 30, 1956.

if $\int_U du = 1$. But a similar statement about f is actually false and a much more delicate investigation of ϕ_f is required. Nevertheless the resemblance in the two cases is so striking that one cannot give up the feeling that they both must be governed by some common principle. However a little closer examination reveals important differences. For example if we replace H by $H' = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and define

$$\phi_f'(t) = t \int_G f(txH')\,dx,$$

we get $\lim_{t\to 0}((d/dt)\phi_f') = 0$. On the other hand in the compact case H is conjugate to $H'' = \begin{pmatrix} (-1)^{\frac{1}{2}} & 0 \\ 0 & -(-1)^{\frac{1}{2}} \end{pmatrix}$ under U and therefore nothing new is obtained if we replace H by H''. This shows that the situation in the noncompact case is considerably more complicated.

Returning to the general case, let $\mathfrak{g}$ be a semisimple Lie algebra over the complex field C. We shall consider the algebra $\mathfrak{D}(\mathfrak{g})$ of polynomial differential operators on $\mathfrak{g}$ (see Section 2 for the precise definition). Let $\mathfrak{g}_0$ and $\mathfrak{u}$ be two real forms of $\mathfrak{g}$ and suppose $\mathfrak{u}$ is compact. It is clear that the complex group G_c of $\mathfrak{g}$ operates on $\mathfrak{D}(\mathfrak{g})$. Hence we can consider the subalgebra $\mathfrak{J}'$ consisting of those elements in $\mathfrak{D}(\mathfrak{g})$ which are invariant under G_c. The structure of $\mathfrak{J}'$ is, of course, completely determined by $\mathfrak{u}$. On the other hand, elements of $\mathfrak{J}'$ can also be regarded as differential operators on $\mathfrak{g}_0$ and therefore the internal structure of $\mathfrak{J}'$ is reflected in the differential equations on $\mathfrak{g}_0$ and this provides the required link from $\mathfrak{u}$ to $\mathfrak{g}_0$. For instance let $\mathfrak{g}$, $\mathfrak{g}_0$ and $\mathfrak{u}$ be as in the above example. Choose complex coordinates x, y, z in $\mathfrak{g}$ such that the corresponding matrix is given by $\begin{pmatrix} z & x \\ y & -z \end{pmatrix}$. Then if the differential operator.

$$D = \partial^2/\partial z^2 + 4\partial^2/\partial x\partial y$$

is interpreted suitably on $\mathfrak{g}_0$ and $\mathfrak{u}$, one finds that $\phi_{Df} = d^2\phi_f/dt^2$ and $\psi_{Dg} = -d^2\psi_g/dt^2$. This is a special case of a result (Lemma 15) which will be proved in its full generality in another paper (see however [4(h)]).

Theorem 1 (Section 3) is the central result of this paper. In Section 5 we give its applications to the case of a compact semisimple Lie algebra. This discussion also enables us to obtain some algebraic results (e.g. Lemma 18) which are valid in the general case as well. Section 8 is devoted to the detailed study of a special case which will have an important significance for later applications. Theorem 5 contains the main result of this section.

2. Preliminary definitions. Let R and C be the fields of real and complex numbers respectively and E_0 a vector space over R of finite dimension. We consider the symmetric algebra [4(c), p. 191] $S(E)$ over the complexification E of E_0. For any $X \in E_0$ let $\partial(X)$ denote the differential operator on E_0 given by[1]

$$f(Y;\partial(X)) = \{(d/dt)f(Y+tX)\}_{t=0} \qquad (Y \in E_0, f \in C^\infty(E_0), t \in R).$$

Then it is obvious that the mapping $X \to \partial(X)$ can be extended uniquely to an algebraic isomorphism of $S(E)$ (over C) into the algebra of differential operators on E_0. Thus for any $p \in S(E)$, we get a differential operator $\partial(p)$ on E. Now suppose there is given a real nondegenerate symmetric bilinear form $B(X,Y)$ $(X, Y \in E_0)$ on E_0. We extend this form on E by linearity (over C) and then use it to identify E with its dual. In this identification an element $X \in E$ corresponds to the linear function $Y \to B(X,Y)$ $(Y \in E)$ and therefore $S(E)$ can now be regarded as the algebra of all polynomial functions on E. In accordance with this intepretation we shall often refer to elements of $S(E)$ as polynomials on E.

Let $\mathcal{E}$ be the algebra of all differential operators on E_0. Then $\mathcal{E} \supset C^\infty(E_0)$, and therefore $S(E)$ and $\partial(S(E))$ are both subalgebras of $\mathcal{E}$. Let $\mathfrak{D}(E)$ denote the subalgebra of $\mathcal{E}$ generated by $S(E) \cup \partial(S(E))$. The elements of $\mathfrak{D}(E)$ will be called polynomial differential operators on E_0. But, whenever convenient, we can regard an element of $\mathfrak{D}(E)$ also as a *holomorphic* differential operator on the *complex* manifold E. Let H be a group of nonsingular linear mappings of E into itself which preserve B so that $B(xX, xY) = B(X,Y)$ $(X, Y \in E; x \in H)$. Then for any $x \in H$, we shall define an automorphism $d \to d^x$ $(d \in \mathfrak{D}(E))$ of $\mathfrak{D}(E)$. In order to do this we have to define $(d^x f)(X_0)$, where f is a holomorphic function on some neighborhood of X_0 in E. If g is a function defined on a subset V of E, let g^x denote the function on xV given by $g^x(X) = g(x^{-1}X)$ $(X \in xV)$. If V is open and g is holomorphic on V, it is clear that g^x is holomorphic on xV. We now define $(d^x f)(X_0) = (df^{x^{-1}})^x(X_0)$. It is easy to check that the operator d^x so defined, is actually a holomorphic differential operator and $d \to d^x$ is a homomorphism of $\mathfrak{D}(E)$ into the algebra of all holomorphic differential operators on E. Moreover if $p \in S(E)$ it is obvious that p^x is the polynomial function $X \to p(x^{-1}X)$ $(X \in E)$ and similarly $(\partial(X))^x = \partial(xX)$. Therefore $(p\partial(q))^x = p^x\partial(q^x)$ $(p, q \in S(E))$. Since every element in $\mathfrak{D}(E)$ is evidently a sum of elements of the form $p\partial(q)$, it follows that $d^x \in \mathfrak{D}(E)$. Finally, the mapping $d \to d^x$ has the inverse $d \to d^{x^{-1}}$ and so it is an automorphism of $\mathfrak{D}(E)$.

---

[1] M being a differentiable manifold (which need not be connected [4(e), (f)]), we denote by $C^\infty(M)$ the space of all (complex-valued) functions on M of class C^∞ and by $C_c(M)$ the space of continuous functions on M which vanish outside some sompact set. If D is a differential operator on M and $f \in C^\infty(M)$, $f(p; D)$ denotes the value of Df at a point p in M (see [4(e), §4]). Moreover $C_c^\infty(M) = C_c(M) \cap C^\infty(M)$.

Let $S_r(E)$ $(r \geqq 0)$ denote the subspace of $S(E)$ spanned by elements of the form $X_1X_2 \cdots X_r$ where $X_i \in E$. (In case $r = 0$, $S_r(E) = C$.) As usual a polynomial on E is said to be homogeneous of degree r if it lies in $S_r(E)$. For any two polynomials p, q let $\langle p, q\rangle$ denote the value of $\partial(p)q$ at zero. It is obvious that if p and q are homogeneous, $\langle p, q\rangle = 0$ unless their degrees are equal. Notice that $\langle X, Y\rangle = B(X, Y)$ $(X, Y \in E)$ and it follows from the symmetry of B that $\langle p, q\rangle = \langle q, p\rangle$. In fact, let $(X_1, \cdots, X_n)$ be a base for E such that[2] $B(X_i, X_j) = \delta_{ij}$. Then if $p = \sum_{m_i \geqq 0} a(m_1, \cdots, m_n)X_1^{m_1}X_2^{m_2} \cdots X_n^{m_n}$ $(a(m_1, \cdots, m_n) \in C)$, it is obvious that

$$\langle X_1^{m_1} \cdots X_n^{m_n}, p\rangle = m_1! \cdots m_n!\, a(m_1, \cdots, m_n).$$

Hence

$$\langle q, p\rangle = \sum m_1! \cdots m_n!\, a(m_1, \cdots, m_n) b(m_1, \cdots, m_n)$$

if $q = \sum b(m_1, \cdots, m_n)X_1^{m_1} \cdots X_n^{m_n}$. This also shows that $\langle p, q\rangle = 0$, for all $q \in S(E)$ implies $p = 0$. Moreover $(\partial(p)q)^x = \partial(p^x)q^x$ and therefore $\langle p^x, q^x\rangle = \langle p, q\rangle$ $(x \in H)$.

Let U be a nonempty open subset of E_0. We shall denote by $\mathscr{B}(U)$ the class of all functions $f \in C^\infty(U)$ such that

$$\nu_d(f) = \sup_{X \in U} |f(X; d)| < \infty$$

for every $d \in \mathfrak{D}(E)$. We topologise $\mathscr{B}(U)$ by means of the seminorms ν_d $(d \in \mathfrak{D}(E))$ and in this way $\mathscr{B}(U)$ becomes a locally convex space. If D is a differential operator on U and X a point in U, it is obvious that there exists a unique element $p \in S(E)$ such that $f(X; D) = f(X; \partial(p))$ for every $f \in C^\infty(U)$. *We call $\partial(p)$ the local expression of D at X. It will usually be denoted by D_X.* Let H_0 be a group of nonsingular linear mappings of E_0 into itself. Then for every function f on U and $x \in H_0$, let f^x denote the function on U given by $f^x(X) = f(x^{-1}X)$ $(X \in U)$. Then corresponding to any differential operator D on U, we define a new differential operator D^x on U by $D^xf = (Df^{x^{-1}})^x$ $(f \in C^\infty(U))$. One proves without difficulty that $(D_X)^x = (D^x)_{xX}$ $(X \in U)$. D is said to be invariant under H_0 if $D^x = D$ for all $x \in H_0$.

---

[2] δ_{ij} is the usual Kronecker symbol. It is equal to 1 or 0 according as $i = j$ or not.

Select a fixed square root of -1 in C and denote it by $(-1)^{\frac{1}{2}}$. Also let dX denote the Euclidean measure on E_0 (normalized in some way). Then for any $f \in \mathcal{C}(E_0)$, the Fourier transform $\bar{f}$ of f is defined as follows.

$$\bar{f}(Y) = \int_{E_0} \exp((-1)^{\frac{1}{2}} B(Y, X)) f(X)\, dX \qquad (Y \in E_0).$$

It is well known [8(I), p. 105] that $\bar{f}$ also lies in $\mathcal{C}(E_0)$ and in fact $f \to \bar{f}$ is a topological mapping of $\mathcal{C}(E_0)$ onto itself. Moreover the measure dX can be so normalized that

$$f(Y) = \int_{E_0} \exp\{-(-1)^{\frac{1}{2}} B(Y, X)\} \bar{f}(X)\, dX \qquad (Y \in E_0)$$

for every $f \in \mathcal{C}(E_0)$. *This normalization will be called the regular normalization.*

LEMMA 1. *There exist a unique automorphism*[3] $d \to \hat{d}$ *of* $\mathfrak{D}(E)$ *such that* $\hat{X} = -(-1)^{\frac{1}{2}} \partial(X)$ *and* $(\partial(X))\hat{} = -(-1)^{\frac{1}{2}} X$ $(X \in E)$. *Moreover* $(df)^{-} = \hat{d}\bar{f}$ *for any* $d \in \mathfrak{D}(E)$ *and* $f \in \mathcal{C}(E_0)$.

Since $\mathfrak{D}(E)$ is generated by $(1, E + \partial(E))$, the uniqueness is obvious. The rest follows immediately from the theory of Fourier transforms [8(I), p. 105].

COROLLARY. *For any* d *in* $\mathfrak{D}(E)$, *we can select another element* $d' \in \mathfrak{D}(E)$ *such that*

$$\int_{E_0} |d\bar{f}|\, dX \leqq \nu_{d'}(f) \qquad (f \in \mathcal{C}(E_0)).$$

Choose a polynomial $p \in S(E)$ such that p is never zero on E_0 and $c = \int_{E_0} |p|^{-1} dX < \infty$. Then if $\phi \in \mathcal{C}(E_0)$,

$$\nu_1(\bar{\phi}) = \sup_{X \in E_0} |\bar{\phi}(X)| \leqq \int_{E_0} |\phi|\, dX \leqq c\nu_1(p\phi).$$

Now it follows from the above lemma that $pd = \hat{d}_1$ for some $d_1 \in \mathfrak{D}(E)$. Hence

$$\int_{E_0} |d\bar{f}|\, dX \leqq c\nu_1(pd\bar{f}) = c\nu_1((d_1 f)^{-}) \leqq c^2\nu(pd_1 f) \qquad (f \in \mathcal{C}(E_0))$$

and so we can take $d' = c^2 p d_1$.

---

[3] We shall write $d\hat{}$, f^{-} respectively instead of $\hat{d}$, $\bar{f}$ whenever it is convenient to do so.

The adjoint of a differential operator D on E_0 is, by definition, the unique differential operator D^* such that

$$\int_{E_0} f(X;D)g(X)dX = \int_{E_0} f(X)g(X;D^*)dX$$

for all $f, g \in C_c^\infty(E_0)$. The mapping $D \to D^*$ is an anti-automorphism of the algebra of all differential operators on E_0 and $(D^*)^* = D$. In particular if p is a homogeneous element in $S(E)$ of degree m, it is obvious that $p^* = p$ and $(\partial(p))^* = (-1)^m \partial(p)$. This shows that $\mathfrak{D}(E))^* = \mathfrak{D}(E)$ and so we get the following result.

LEMMA 2. *There exists a unique anti-automorphism* $d \to d^*$ *of* $\mathfrak{D}(E)$ *such that* $p^* = p$ *and* $(\partial(p))^* = (-1)^m \partial(p)$ *for any homogeneous polynomial in* $S(E)$ *of degree* m.

Again the uniqueness follows from the fact that $\mathfrak{D}(E)$ is generated by $S(E) \cup \partial(S(E))$.

U and H_0 being as before, let τ denote a distribution on U [8(I)] and dX the Euclidean measure on E_0. Then, if F is a measurable and locally summable function on U, we say that[4] $\tau = F$ if

$$\tau(f) = \int_U fF\,dX$$

for every $f \in C_c^\infty(U)$. Let V be a subset of $C_c^\infty(U)$. Then by the C_c^∞-topology on V, we mean the topology induced under the usual topology of $C_c^\infty(U)$ [8(I), p. 67]. Similarly if V' is a subset of $\mathcal{E}(U)$, the $\mathcal{E}$-topology on V' is the one induced on it by $\mathcal{E}(U)$. A distribution τ on E_0 will be called a $\mathcal{E}$-distribution if it is continuous under the $\mathcal{E}$-topology on $C_c^\infty(E_0)$. In case this is so, τ can be extended uniquely to a continuous function on $\mathcal{E}(E_0)$ [8(II, pp. 93-94]. If D is a differential operator and τ a distribution on U, the mapping $f \to \tau(D^*f)$ $(f \in C_c^\infty(U))$, where D^* is the adjoint of D, is also a distribution and it will be denoted by $D\tau$. If τ is continuous with respect to the $\mathcal{E}$-topology, the same holds for $D\tau$ provided $D \in \mathfrak{D}(E)$. τ is said to be invariant under H_0 if $\tau(f^x) = \tau(f)$ for all $f \in C_c^\infty(U)$ and $x \in H_0$. More generally, a $\mathcal{E}$-distribution τ on U is a continuous linear mapping of $\mathcal{E}(U)$ into C. If $D \in \mathfrak{D}(E)$, the mapping $D\tau: f \to \tau(D^*f)$ $(f \in \mathcal{E}(U))$ is also a $\mathcal{E}$-distribution on U.

We now introduce a notation which will be used rather frequently. Let M_1, M_2 be two manifolds and f a function on $M_1 \times M_2$ of class C^∞.

---

[4] Of course this definition depends on the normalization of dX.

Then if $m_i \in M_i$ and D_i is a differential operator on M_i $(i=1,2)$, we shall denote the value of $(D_1 \times D_2)f$ at (m_1, m_2) by $f(m_1;D_1:m_2;D_2)$. Moreover D_i will be suppressed in this notation whenever it is 1. For example $f(m_1:m_2;D_2)=f(m_1;1:m_2;D_2)$.

Now suppose F is the complexication in E of a vector subspace F_0 of E. Then $S(F) \subset S(E)$. Let B_F denote the restriction of the bilinear form B on F and suppose B_F is nondegenerate. Then we can identify F with its dual under B_F and thus regard $S(F)$ as the algebra of all polynomial functions on F. For any function f on E_0, let $\bar{f}$ denote its restriction on F_0. Then if $f \in S(E)$, it is clear that $\bar{f}$ is a polynomial function[5] on F_0 and therefore it lies in $S(F)$. Moreover if $f \in S(F)$, $f=\bar{f}$ in $S(E)$. Similarly $\partial(S(F)) \subset \partial(S(E))$ and therefore $\mathfrak{D}(F) \subset \mathfrak{D}(E)$. Elements of $\mathfrak{D}(F)$ can therefore be regarded as differential operators either on F_0 or E_0. But in view of the relation $\overline{df}=d\bar{f}$ $(f \in C^\infty(E_0), d \in \mathfrak{D}(F))$, it is not necessary to distinguish between the two meanings. Also it follows from Lemma 2 that the adjoint operation in $\mathfrak{D}(E)$ coincides on $\mathfrak{D}(F)$ with the corresponding operation in $\mathfrak{D}(F)$. The same obviously holds for the scalar product $\langle p, q\rangle$ $(p, q \in S(F))$.

3. Invariant differential operators. Let $\mathfrak{g}_0$ be a semisimple Lie algebra over R and $\mathfrak{h}_0$ a Cartan subalgebra of $\mathfrak{g}_0$. We denote the corresponding complexifications by $\mathfrak{g}$ and $\mathfrak{h}$ respectively. Then if we take $E_0=\mathfrak{g}_0$, $F_0=\mathfrak{h}_0$ and[6] $B(X,Y)=\mathrm{sp}(\mathrm{ad}\,X\,\mathrm{ad}\,Y)$ $(X, Y \in \mathfrak{g}_0)$, all the above conditions are fulfilled. Let G be the (connected) adjoint group of $\mathfrak{g}_0$. Then every $x \in G$ can be regarded as a nonsingular linear transformation of $\mathfrak{g}$ which preserves B and so it defines an automorphism $D \rightarrow D^x$ $(D \in \mathfrak{D}(E))$ of $\mathfrak{D}(E)$. We call a function f of $\mathfrak{g}_0$ invariant (under G) if $f^x=f$ $(x \in G)$. Let $I(\mathfrak{g})$ be the set of invariant elements in $S(\mathfrak{g})$. Then, if f is an invariant function in $C^\infty(\mathfrak{g}_0)$ and $p \in I(\mathfrak{g})$, it is obvious that $\partial(p)f$ is also invariant. We would like to express $\overline{\partial(p)f}$ in terms of $\partial(\bar{p})$ and $\bar{f}$ (where the bar denotes restriction on $\mathfrak{h}_0$). Let $\alpha_1, \cdots, \alpha_r$ be all the distinct positive roots of $\mathfrak{g}$ (with respect to $\mathfrak{h}$) under some fixed order (see [4(g), §2]). Then $\pi=\alpha_1\alpha_2\cdots\alpha_r$ is a polynnomial function on $\mathfrak{h}$. we intend to prove that $\pi\overline{\partial(p)f}=\partial(\bar{p})(\pi\bar{f})$.

First we introduce some notation. Let U be an open subset of $\mathfrak{g}_0$.

---

[5] We agree to identify a polynomial function on E with its restriction on E_0. Similarly for F.

[6] $X \rightarrow \mathrm{ad}\,X$ $(X \in \mathfrak{g})$ denotes the adjoint representation of $\mathfrak{g}$.

Select open subsets $\mathfrak{g}_1$, G_1 of $\mathfrak{g}_0$ and G respectively such that $xX \in U$ for $x \in G_1$, $X \in \mathfrak{g}_1$. For any $f \in C^\infty(U)$, consider the function

$$g(x:X) = f(xX) \qquad (x \in G_1, X \in \mathfrak{g}_1)$$

on $G_1 \times \mathfrak{g}_1$. If d and D are differential operators on G_1 and $\mathfrak{g}_1$ respectively, we put $f(x;d:X;D) = g(x;d:X;D)$. (Again we suppress d or D whenever it is 1.) Let $\mathfrak{B}$ be the universal enveloping algebra of $\mathfrak{g}$. Then elements of $\mathfrak{B}$ can be regarded as left-invariant differential operators on G [4(e), §4]. All products of the form $X_1^{m_1} \cdots X_r^{m_r}$ $(X_i \in \mathfrak{g})$ are meant to be in $S(\mathfrak{g})$ unless it is explicitly stated otherwise. Now suppose $Y \in \mathfrak{g}_1$, $p \in S(\mathfrak{g})$ and $f \in C^\infty(U)$. Then

$$f(x:Y;\partial(p)) = f(xY;\partial(p^x)) \qquad (x \in G_1)$$

and therefore if $X \in \mathfrak{g}_0$,

$$f(x;X:Y;\partial(p)) = \{(d/dt)f(x_tY;\partial(p^{x_t}))\}_{t=0} \qquad (t \in R)$$

where $x_t = x \exp tX$. For any $Z \in \mathfrak{g}$, let d_Z denote the derivation of $S(\mathfrak{g})$ which coincides with $\operatorname{ad} Z$ on $\mathfrak{g}$. It is clear that

$$\{(d/dt)f(x_tY;\partial(p^{x_t}))\}_{t=0} = \{(d/dt)f(x_tY;\partial(p^x))\}_{t=0} + \{(d/dt)f(xY;\partial(p^{x_t}))\}_{t=0}$$

and

$$f(x_tY;\partial(p^x)) = f(x:z_tY;\partial(p)),\ f(xY;\partial(p^{x_t})) = f(x:Y;\partial(p^{z_t})),$$

where $z_t = \exp tX$. Hence

$$f(x;X:Y;\partial(p)) = f(x:Y;\partial((d_XY)p + d_Xp)).$$

For any $q \in S(\mathfrak{g})$, let L_q denote the linear mapping $p \to qp$ $(p \in S(\mathfrak{g}))$ of $S(\mathfrak{g})$. Then we have the following result.

LEMMA 3. *Let $f \in C^\infty(U)$, $X_1, \cdots, X_r \in \mathfrak{g}$ and $p \in S(\mathfrak{g})$. Moreover let $\cdot$ denote multiplication in $\mathfrak{B}$. Then if $Y \in \mathfrak{g}_1$,*

$$f(x;X_1 \cdot X_2 \cdot \cdots \cdot X_r:Y;\partial(p)) = f(x:Y;\partial(q)) \qquad (x \in G_1),$$

where[7]

$$q = (L_{[X_1,Y]} + d_{X_1})(L_{[X_2,Y]} + d_{X_2}) \cdots (L_{[X_r,Y]} + d_{X_r})p.$$

For $r = 1$ this has been proved above. So now suppose $r > 1$ and use induction. Put

$$q' = (L_{[X_2,Y]} + d_{X_2}) \cdots (L_{[X_r,Y]} + d_{X_r})p.$$

---

[7] $[X,Y] = d_XY$ $(X, Y \in \mathfrak{g})$ as usual.

Then by induction hypothesis

$$f(x';X_2\cdot\cdots\cdot X_r:Y;\partial(p))=f(x':Y;\partial(q')) \qquad (x'\in G_1).$$

Hence $f(x;X_1\cdot X_2\cdot\cdots\cdot X_r:Y;\partial(p))$

$$=\{(d/dt)f(x\exp tX_1;X_2\cdot\cdots\cdot X_r:Y;\partial(p))\}_{t=0}$$

$$=\{(d/dt)f(x\exp tX_1:Y;\partial(q'))\}_{t=0}$$

$$=f(x;X_1:Y;\partial(q'))=f(x:Y;\partial((L_{[X_1,Y]}+d_{X_1})q')))$$

$=f(x:Y;\partial(q))$. This proves the lemma.

Now consider the tensor product $\mathfrak{B}\times S(\mathfrak{g})$. The above lemma shows[8] that for every $Y\in\mathfrak{g}_0$ there exists a unique bilinear mapping Γ_Y of $\mathfrak{B}\times S(\mathfrak{g})$ into $S(\mathfrak{g})$ such that $\Gamma_Y(1\times p)=p$ and

$$\Gamma_Y(X_1\cdot X_2\cdot\cdots\cdot X_r\times p)=(L_{[X_1,Y]}+d_{X_1})\cdots(L_{[X_r,Y]}+d_{X_r})p$$

$(X_1,\cdots,X_r\in\mathfrak{g};p\in S(\mathfrak{g}))$. For any root α (of $\mathfrak{g}$ with respect to $\mathfrak{h}$), select an element $X_\alpha\neq 0$ in $\mathfrak{g}$ such that $[H,X_\alpha]=\alpha(H)X_\alpha$ for all $H\in\mathfrak{h}$. Put $\mathfrak{s}=\sum_\alpha CX_\alpha$ where α runs over all the roots. Then the symmetric algebra $S(\mathfrak{s})$ over $\mathfrak{s}$ is a subalgebra of $S(\mathfrak{g})$. Let λ denote the canonical mapping [4(c), p. 192] of $S(\mathfrak{g})$ into $\mathfrak{B}$ and put $\mathfrak{S}=\lambda(S(\mathfrak{s}))$.

LEMMA 4. *Let H_0 be an element in $\mathfrak{h}_0$ such that $\pi(H_0)\neq 0$. Then Γ_{H_0} defines a one-one mapping of $\mathfrak{S}\times S(\mathfrak{h})$ onto $S(\mathfrak{g})$.*

Let $S_d(\mathfrak{g})$, $S_d(\mathfrak{s})$ and $S_d(\mathfrak{h})$ denote the spaces of homogeneous elements of degree d in $S(\mathfrak{g})$, $S(\mathfrak{s})$ and $S(\mathfrak{h})$ respectively and put $\mathfrak{S}_d=\lambda(S_d(\mathfrak{s}))$. We shall prove by induction on r that

$$\sum_{d+e\leqq r}\Gamma_{H_0}(\mathfrak{S}_d\times S_e(\mathfrak{h}))=\sum_{s\leqq r}S_s(\mathfrak{g}).$$

This is obvious if $r=0$. So now suppose $r\geqq 1$. It is clear that the left side is contained in the right side. Hence in view of our induction hypothesis it is enough to prove that

$$\sum_{d+e\leqq r}\Gamma_{H_0}(\mathfrak{S}_d\times S_e(\mathfrak{h}))+\mathscr{S}_{r-1}\supset S_r(\mathfrak{g}),$$

where $\mathscr{S}_k=\sum_{s\leqq k}S_s(\mathfrak{g})$. Since $\mathfrak{g}=\mathfrak{h}+\mathfrak{s}$, $S_r(\mathfrak{g})$ is spanned by elements of the form $Z_1Z_2\cdots Z_dH_1H_2\cdots H_e$ $(Z_i\in\mathfrak{S},H_j\in\mathfrak{h})$, where $d+e=r$. Moreover the restriction of $\mathrm{ad}\,H_0$ on $\mathfrak{s}$ is nonsingular since $\pi(H_0)\neq 0$. Therefore we can select $Y_i\in\mathfrak{s}$ such that $[H_0,Y_i]=-Z_i$ $1\leqq i\leqq d$. Then

---

[8] The proof of this fact is exactly parallel to that of Lemma 15 of [4(e)].

$$\begin{aligned}\Gamma_{H_0}(Y_1\cdot Y_2\cdot\cdots\cdot Y_d\mathbf{X}H_1\cdots H_e)&=(L_{Z_1}+d_{Y_1})\cdots(L_{Z_d}+d_{Y_d})(H_1\cdots H_e)\\&\equiv Z_1Z_2\cdots Z_dH_1\cdots H_e \bmod \mathcal{S}_{r-1}.\end{aligned}$$

On the other hand $Y_1\cdot Y_2\cdot\cdots\cdot Y_d-\lambda(Y_1Y_2\cdots Y_d)\in\lambda(\mathcal{S}_{d-1})$ (see [4(a)]) and $\Gamma_{H_0}(\lambda(\mathcal{S}_{d-1})\mathbf{X}H_1\cdots H_e)\subset\mathcal{S}_{d+e-1}=\mathcal{S}_{r-1}$. Hence it follows that

$$\Gamma_{H_0}(\lambda(Y_1\cdots Y_d)\mathbf{X}H_1H_2\cdots H_e)-(Z_1Z_2\cdots Z_dH_1\cdots H_e)\in\mathcal{S}_{r-1}$$

and this proves our assertion. Now the spaces $\mathcal{S}_r$ and $\sum_{d+e\leqq r}\mathfrak{S}_d\mathbf{X}S_e(\mathfrak{h})$ have the same dimension from Lemma 12 of [4(c)]. Therefore Γ_{H_0} must be one-one.

Let U and V be two vector spaces over C and suppose the dimension of U is finite. A mapping f of U into V will be called a polynomial mapping if (1) the subspace of V spanned by $f(U)$ is of finite dimension and (2) for every linear function μ on V, $u\to\mu(f(u))$ $(u\in U)$ is a polynomial function on U.

LEMMA 5. *For every $p\in S(\mathfrak{g})$ there exists an integer $r\geqq 0$ and a polynomial mapping γ_p of $\mathfrak{h}$ into $\mathfrak{S}\mathbf{X}S(\mathfrak{h})$ such that $\Gamma_H(\gamma_p(H))=\pi(H)^rp$ $(H\in\mathfrak{h}_0)$.*

This is proved in substantially the same way as Lemma 16 of [4(e)].

Now put $\mathfrak{S}'=\sum_{d\geqq 1}\mathfrak{S}_d$ and let $\mathfrak{h}_0'$ denote the set of all $H\in\mathfrak{h}_0$ where $\pi(H)\neq 0$. It follows from Lemma 4 that for any $H\in\mathfrak{h}_0'$ and $p\in S(\mathfrak{g})$, there exists a unique element $\beta_H(p)\in S(\mathfrak{h})$ such that $p-\beta_H(p)\in\Gamma_H(\mathfrak{S}'\mathbf{X}S(\mathfrak{h}))$. Hence we can define a mapping $\delta_H'(H\in\mathfrak{h}_0')$ of $\partial(S(\mathfrak{g}))$ into $\partial(S(\mathfrak{h}))$ by $\delta_H'(\partial(p))=\partial(\beta_H(p))$ $(p\in S(\mathfrak{g}))$. We extend this to a mapping of $\mathfrak{D}(\mathfrak{g})$ into $\partial(S(\mathfrak{g}))$ by setting $\delta_H'(D)=\delta_H'(D_H)$ $(D\in\mathfrak{D}(\mathfrak{g}))$ where D_H is the local expression of D at H. Then it follows from Lemma 5 that there exists an integer $m\geqq 0$ and a polynomial mapping γ of $\mathfrak{h}$ into $\partial(S(\mathfrak{h}))$ such that $\delta_H'(D)=\pi(H)^{-m}\gamma(H)$ $(H\in\mathfrak{h}_0')$. This shows that there exists a differential operator $\delta'(D)$ on $\mathfrak{h}_0'$ whose local expression at any point $H\in\mathfrak{h}_0'$ coincides with $\delta_H'(D)$. The significance of $\delta'(D)$ is given by the following lemma.

LEMMA 6. *Let U be an open neighborhood in $\mathfrak{g}_0$ of a point $H\in\mathfrak{h}_0'$. Suppose f is a function in $C^\infty(U)$ and $f(xX)=f(X)$ whenever (x,X) is sufficiently near $(1,H)$ in $G\times\mathfrak{g}_0$. Then if $\bar{f}$ denotes the restriction of f on $U\cap\mathfrak{h}_0'$, $f(H;D)=\bar{f}(H;\delta'(D))$ for $D\in\mathfrak{D}(\mathfrak{g})$.*

Select $p\in S(\mathfrak{g})$ such that $D_H=\partial(p)$. Then we know that

$$p=\Gamma_H(1\mathbf{X}\beta_H(p))+\sum_{i=1}^{r}s_i\mathbf{X}h_i$$

where $s_i \in \mathfrak{S}'$ and $h_i \in S(\mathfrak{h})$. Therefore from Lemma 5,

$$f(x:H;\partial(p)) = f(x:H;\partial(\beta_H(p))) + \sum_{i=1}^{r} f(x;s_i:H;\partial(h_i)),$$

if x lies sufficiently near 1 in G. But it is obvious from our assumption on f that $f(x;b:X) = 0$ $(b \in \mathfrak{B}\mathfrak{g})$ if (x,X) is sufficiently near $(1,H)$ in $G \times \mathfrak{g}_0$. Hence $f(x:H;\partial(p)) = f(x:H;\partial(\beta_H(p)))$. But $\partial(p) = D_H$ and $\partial(\beta_H(p)) = \delta_H'(D_H) = \delta_H'(D)$. Therefore putting $x = 1$, we get $f(H;D) = f(H;\delta_H'(D))$, which is equivalent to the assertion of the lemma.

Let $\mathfrak{J}'$ be the subalgebra consisting of those elements $D \in \mathfrak{D}(\mathfrak{g})$ which are invariant under G.

LEMMA 7. *The mapping $D \rightarrow \delta'(D)$ $(D \in \mathfrak{J}')$ is a homomorphism of $\mathfrak{J}'$ into the algebra of all differential operators on $\mathfrak{h}_0'$.*

Let H_0 be a point in $\mathfrak{h}_0'$ and A the Cartan subgroup of G (see [4(e), §2]) corresponding to $\mathfrak{h}_0$. Let $x \rightarrow x^*$ denote the natural mapping of G on $G^* = G/A$ and put $x^*H = xH$ $(x \in G, H \in \mathfrak{h}_0)$. Select open connected neighborhoods U and V of H_0 and 1 in $\mathfrak{h}_0'$ and G respectively. Let V^* be the image of V in G^*. Then the mapping ϕ: $(x^*,H) \rightarrow x^*H$ of $V^* \times U$ into $\mathfrak{g}_0$ is easily seen to be regular (see [4(d), p. 501]). Therefore since the two manifolds $V^* \times U$ and $\mathfrak{g}_0$ have the same dimension, $N = \phi(V^* \times U)$ is an open submanifold of $\mathfrak{g}_0$. Moreover it follows that if V and U are sufficiently small, ϕ is univalent and therefore it defines an analytic isomorphism of $V^* \times U$ onto N. For any $g \in C^\infty(U)$, let f_g denote the function in $C^\infty(N)$ given by $f_g(\phi(x^*,H)) = g(H)$ $(x^* \in V^*, H \in U)$. Then $f_g(xH) = g(H)$ $(x \in V, H \in U)$. Now suppose $D_1, D_2 \in \mathfrak{J}'$ and put $F = D_2 f_g$. Since D_2 is invariant under G, it is clear that Lemma 6 is applicable to F and therefore $F(H;D_1) = \bar{F}(H;\delta'(D_1))$ $(H \in U)$. On the other hand by applying the same lemma to f_g we get

$$\bar{F}(H) = f_g(H;D_2) = g(H;\delta'(D_2)) \qquad (H \in U).$$

Therefore, $f_g(H;D_1D_2) = F(H;D_1) = \bar{F}(H;\delta'(D_1)) = g(H;\delta'(D_1)\delta'(D_2))$. But again from Lemma 6, $f_g(H;D_1D_2) = g(H;\delta'(D_1D_2))$. Therefore, $g(H;\delta'(D_1D_2)) = g(H;\delta'(D_1)\delta'(D_2))$ and this proves that $\delta'(D_1D_2) = \delta'(D_1)\delta'(D_2)$ on U. But since U is a neighborhood of an arbitrary point $H_0 \in \mathfrak{h}_0'$, we conclude that $\delta'(D_1D_2) = \delta'(D_1)\delta'(D_2)$ on $\mathfrak{h}_0'$.

We recall that $I(\mathfrak{g}) = S(\mathfrak{g}) \cap \mathfrak{J}'$. Let $\mathfrak{J}(\mathfrak{g})$ be the subalgebra of $\mathfrak{J}'$ generated by $I(\mathfrak{g}) \cup \partial(I(\mathfrak{g}))$. We shall now determine $\delta'(D)$ for $D \in \mathfrak{J}(\mathfrak{g})$. Obviously, if $p \in I(\mathfrak{g})$, $\delta'(p) = \bar{p}$, where $\bar{p}$ is the restriction of p on $\mathfrak{h}$.

Therefore in view of Lemma 7, it is sufficient to determine $\delta'(D)$ for $D \in \partial(I(\mathfrak{g}))$.

LEMMA 8. *If* $p \in I(\mathfrak{g})$ *then*[9] $\delta'(\partial(p)) = \pi^{-1}\partial(\bar{p}) \circ \pi$.

Define a polynomial function ω on $\mathfrak{g}$ by $\omega(X) = \mathrm{sp}(\mathrm{ad}\, X)^2$ $(X \in \mathfrak{g})$. (We shall call ω the Casimir polynomial of $\mathfrak{g}$.) Then $\omega \in I(\mathfrak{g})$ and we shall first compute $\delta'(\omega)$. Let P be the set of all positive roots. For any $\alpha \in P$, normalize the elements X_α, $X_{-\alpha}$ in such a way that $B(X_\alpha, X_{-\alpha}) = 1$ and put $H_\alpha = [X_\alpha, X_{-\alpha}]$. Then $B(H_\alpha, H) = \alpha(H)$ $(H \in \mathfrak{h})$ and therefore $\alpha = H_\alpha$ under our identification of $\mathfrak{h}$ with its dual. Now consider the polynomial function

$$\xi = \omega - \bar{\omega} - 2 \sum_{\alpha \in P} X_\alpha X_{-\alpha}.$$

If $X = \mathrm{H} + \sum_{\alpha \in P} (c_\alpha X_\alpha + c_{-\alpha} X_{-\alpha})$ $(H \in \mathfrak{h}, c_\alpha, c_{-\alpha} \in C)$, it is clear that

$$\omega(X) = \mathrm{sp}(\mathrm{ad}\, X)^2 = \mathrm{sp}(\mathrm{ad}\, H)^2 + 2 \sum_{\alpha \in P} c_{-\alpha} c_\alpha.$$

Therefore, since $B(X, X_\beta) = c_{-\beta}$ for any root β, it follows that $\xi(X) = 0$. Hence $\omega = \bar{\omega} + 2 \sum_{\alpha \in P} X_\alpha X_{-\alpha}$. Now if $H \in \mathfrak{h}_0'$,

$$\Gamma_{H_0}((X_\alpha \cdot X_{-\alpha}) \mathbf{X}\, 1) = (L_{[X_\alpha, H_0]} + d_{X_\alpha})[X_{-\alpha}, H] = \alpha(H_0) X_\alpha X_{-\alpha} - \alpha(H_0) H_\alpha$$

and $X_\alpha \cdot X_{-\alpha} = \frac{1}{2}(X_\alpha \cdot X_{-\alpha} + X_{-\alpha} \cdot X_\alpha) + \frac{1}{2} H_\alpha$ in $\mathfrak{B}$. Hence

$$\Gamma_{H_0}\Big(\sum_{\alpha \in P} \alpha(H_0)^{-2}(X_\alpha \cdot X_{-\alpha} + X_{-\alpha} \cdot X_\alpha) \mathbf{X}\, 1 + (1 \mathbf{X}\, \bar{\omega}) + 2 \sum_{\alpha \in P} \alpha(H_0)^{-1}(1 \mathbf{X}\, H_\alpha)\Big)$$

$= \bar{\omega} + 2 \sum_{\alpha \in P} X_\alpha X_{-\alpha} = \omega$. This proves that

$$\delta_{H_0}'(\partial(\omega)) = \partial(\bar{\omega}) + 2 \sum_{\alpha \in P} \alpha(H_0)^{-1} \partial(H_\alpha)$$

since $X_\alpha \cdot X_{-\alpha} + X_{-\alpha} \cdot X_\alpha \in \mathfrak{S}'$. On the other hand let us compute $\pi^{-1}\partial(\bar{\omega}) \circ \pi$. For any two differential operators D_1, D_2 put $\{D_1, D_2\} = D_1 \circ D_2 - D_2 \circ D_1$. Then, if $\alpha_1, \cdots, \alpha_r$ are all the distinct positive roots,

$$\{\partial(\bar{\omega}), \pi\} = \sum_{k=1}^{r} \alpha_1 \alpha_2 \cdots \alpha_{k-1} \{\partial(\bar{\omega}), \alpha_k\} \circ (\alpha_{k+1} \cdots \alpha_r).$$

Moreover a simple calculation shows[10] that $\{\partial(\bar{\omega}), \alpha\} = 2\partial(H_\alpha)$. Therefore

$$\partial(\bar{\omega}) \circ \pi = \pi \partial(\bar{\omega}) + 2 \sum_{k=1}^{r} \alpha_1 \alpha_2 \cdots \alpha_{k-1} \partial(H_{\alpha_k}) \circ (\alpha_{k+1} \cdots \alpha_r).$$

---

[9] Whenever it is necessary to avoid confusion, we denote the product of two differential operators D_1, D_2 by $D_1 \circ D_2$.

[10] This is best done by making use of a base $H_1, \cdots, H_l$ for $\mathfrak{h}$ such that $B(H_i, H_j) = \delta_{ij}$ $(1 \leqq i, j \leqq l)$.

But $\{\partial(H_\alpha), \beta\} = \beta(H_\alpha)$ for any two roots α, β, and so we can conclude that

$$\partial(\bar{\omega}) \circ \pi = \pi \partial(\bar{\omega}) + 2 \sum_{k=1}^{r} \alpha_k^{-1} \partial(H_{\alpha_k}) + q,$$

where $q \in S(\mathfrak{h})$. Applying both sides of the above equation to the constant function 1, we find that $q = \partial(\bar{\omega})\pi$. But we shall see presently (Lemma 9 and the Corollary to Lemma 10) that $\partial(\bar{\omega})\pi = 0$. Therefore by comparing this with our earlier expression for $\delta_{H_0}'(\partial(\omega))$, it follows that $\delta'(\partial(\omega)) = \pi^{-1} \partial(\bar{\omega}) \circ \pi$. This proves our assertion in case $p = \omega$.

Now let μ be the derivation of $\mathfrak{D}(\mathfrak{g})$ given by $\mu D = \frac{1}{2}\{\partial(\omega), D\}$ $(D \in \mathfrak{D}(\mathfrak{g}))$. A direct computation shows that $\mu X = \partial(X)$ $(X \in \mathfrak{g})$. We shall now prove by induction on m that $\mu^m(X_1 X_2 \cdots X_m) = m!\,\partial(X_1 X_2 \cdots X_m)$ for $X_1, \cdots, X_m \in \mathfrak{g}$. Since $\mu^2 X = \mu\partial(X) = 0$ $(X \in \mathfrak{g})$, it follows from the Leibnitz rule for derivations that

$$\mu^m(X_1 X_2 \cdots X_m) = (\mu^m(X_1 \cdots X_m)) \circ X_m + m\mu^{m-1}(X_1 \cdots X_{m-1}) \circ \mu X_m.$$

But $\mu^{m-1}(X_1 \cdots X_{m-1}) = (m-1)!\,\partial(X_1 X_2 \cdots X_{m-1})$ by induction hypothesis. Therefore $\mu^m(X_1 \cdots X_{m-1}) = 0$ and

$$\mu^m(X_1 X_2 \cdots X_m) = m!\,\partial(X_1 \cdots X_{m-1}) \circ \mu X_m = m!\,\partial(X_1 \cdots X_{m-1} X_m).$$

This shows that if q is a homogeneous element in $S(\mathfrak{g})$ of degree m, then $\mu^m q = m!\,\partial(q)$.

On the other hand let us put $\bar{\mu}\xi = \frac{1}{2}\{\delta'(\omega), \xi\}$ for any differential operator ξ on $\mathfrak{h}_0'$. Then $\bar{\mu}$ is a derivation of the algebra of differential operators on $\mathfrak{h}_0'$ and it follows from Lemma 7 that $\delta'(\mu D) = \bar{\mu}\delta'(D)$ for $D \in \mathfrak{J}'$. Let p be a homogeneous element in $I(\mathfrak{g})$ of degree m. Since $\mathfrak{J}'$ is obviously stable under μ, we conclude that

$$m!\,\delta'(\partial(p)) = \delta'(\mu^m p) = \bar{\mu}^m \delta'(p) = \bar{\mu}^m \bar{p}.$$

Now let $\mathfrak{A}$ be an associative algebra and for any $a \in \mathfrak{A}$, let d_a denote the derivation of $\mathfrak{A}$ defined by $d_a b = \frac{1}{2}(ab - ba)$ $(b \in \mathfrak{A})$. Then one proves easily by induction on k that

$$d_a^k b = 2^{-k} \sum_{0 \leqq r \leqq k} C_r^k (-1)^r a^{k-r} b a^r \qquad (k \geqq 0).$$

We now suppose that $\mathfrak{A}$ has a unit element, c is an element in $\mathfrak{A}$ with an inverse c^{-1} and $a' = c^{-1}ac$. Then if $b \in \mathfrak{A}$ and it commutes with c, it is clear that

$$d_{a'}^k b = c^{-1}(d_a^k b) c \qquad (k \geqq 0).$$

Let us now take $\mathfrak{A}$ to be the algebra of all differential operators on $\mathfrak{h}_0'$. Then if $a = \partial(\bar\omega)$, $b = \bar p$ and $c = \pi$, all the above conditions are fulfilled and $a' = \pi^{-1}\partial(\bar\omega)\circ\pi = \delta'(\omega)$ as we have seen above. Moreover if q is any homogeneous element in $S(\mathfrak{h})$ of degree k, we prove in the same way as above that $d_a{}^k q = k!\,\partial(q)$. Therefore

$$\mu^m \bar p = d_{a'}{}^m \bar p = \pi^{-1}(d_a{}^m \bar p)\circ\pi = m!\,\pi^{-1}\partial(\bar p)\circ\pi$$

and this proves that $\delta'(\partial(p)) = \pi^{-1}\partial(\bar p)\circ\pi$ for any homogeneous element $p \in I(\mathfrak{g})$. But it is obvious that $I(\mathfrak{g}) = \sum_{m\geqq 0} I(\mathfrak{g}) \cap S_m(\mathfrak{g})$ and so the assertion of the lemma follows.

Let W denote the Weyl group of $\mathfrak{g}$ with respect to $\mathfrak{h}$ (see [4(b), p. 29]). Then W is a group of nonsingular linear mappings of $\mathfrak{h}$ and therefore (see Section 2) it operates on $\mathfrak{D}(\mathfrak{h})$. Let $\mathfrak{I}(\mathfrak{h})$ denote the subalgebra of those elements in $\mathfrak{D}(\mathfrak{h})$ which are invariant under W.

THEOREM 1. *There exists a unique homomorphism* δ *of* $\mathfrak{I}(\mathfrak{g})$ *into* $\mathfrak{I}(\mathfrak{h})$ *such that* $\delta(p) = p$ *and* $\delta(\partial(p)) = \partial(\bar p)$ $(p \in I(\mathfrak{g}))$. *Moreover* $\delta'(D) = \pi^{-1}\delta(D)\circ\pi$ *on* $\mathfrak{h}_0'$ *for any* $D \in \mathfrak{I}(\mathfrak{g})$.

Since $\mathfrak{I}(\mathfrak{g})$ is generated by $I(\mathfrak{g}) \cup \partial(I(\mathfrak{g}))$, the uniqueness of δ is obvious. Let $\mathfrak{H}'$ denote the algebra of all differential operators on $\mathfrak{h}_0'$. It is clear that we can regard $\mathfrak{D}(\mathfrak{h})$ as a subalgebra of $\mathfrak{H}'$. Put $\delta(D) = \pi\delta'(D)\circ\pi^{-1}$. Then it follows from Lemma 7, that δ is a homomorphism of $\mathfrak{I}(\mathfrak{g})$ into $\mathfrak{H}'$. Moreover $\delta(p) = \bar p$, $\delta(\partial(p)) = \partial(\bar p)$ $(p \in I(\mathfrak{g}))$ from Lemma 8 and $\bar p$ is invariant under W (see Lemma 9 below). Therefore it is obvious that δ maps $\mathfrak{I}(\mathfrak{g})$ into $\mathfrak{I}(\mathfrak{h})$ and so the theorem is proved.

4. Invariants of the Weyl group. An element $q \in S(\mathfrak{h})$ is said to be invariant (under W) if $q^s = q$ for all $s \in W$. Let $I(\mathfrak{g})$ be the subalgebra of $S(\mathfrak{h})$ consisting of all invariants. The following result is due to Chevalley (see [1, exposé 19, p. 10]).

LEMMA 9 (Chevalley). *If* $p \in I(\mathfrak{g})$, *then* $\bar p \in I(\mathfrak{h})$, *and* $p \to \bar p$ *is an isomorphism of* $I(\mathfrak{g})$ *onto* $I(\mathfrak{h})$.

For any root α let s_α denote the Weyl reflexion corresponding to α. An element $q \in S(\mathfrak{h})$ will be called skew (or skew-invariant) if $q^{s_\alpha} = -q$ for every root α. It is known (see Weyl [9]) that π is skew.

LEMMA 10. *If* q *is a skew-invariant in* $S(\mathfrak{h})$, *then* $q = \pi q_0$ *for some* $q_0 \in I(\mathfrak{h})$.

For any root α, let σ_α denote the hyperplane in $\mathfrak{h}$ given by the equation $\alpha=0$. Then if $p \in S(\mathfrak{h})$, it follows from the definition of s_α that $p^{s_\alpha}-p$ vanishes everywhere on σ_α. Therefore $p^{s_\alpha}-p$ is divisible by α in the polynomial ring $S(\mathfrak{h})$. This shows that $q=-\frac{1}{2}(q^{s_\alpha}-q)$ is divisible by α. Now the hyperplanes σ_α corresponding to distinct positive roots α are distinct. Therefore since $S(\mathfrak{h})$ is a unique factorization domain, q is divisible by $\prod_{\alpha \in P} \alpha=\pi$. This means that $q=\pi q_0$, where $q_0 \in S(\mathfrak{h})$. But since both π and q are skew, it follows that $q_0{}^{s_\alpha}=q_0$ $(\alpha \in P)$. Therefore since W is generated by the reflexions s_α $(\alpha \in P)$, we conclude that $q_0 \in I(\mathfrak{h})$.

COROLLARY. *If q is a homogeneous element in $I(\mathfrak{h})$ of positive degree, then $\partial(q)\pi=0$.*

Let r be the degree of π. Then it is obvious that $\partial(q)\pi$ is homogeneous and its degree is lower than r. On the other hand, since $q \in I(\mathfrak{h})$, it is clear that $\partial(q)\pi$ is a skew-invariant. Therefore in view of the above lemma, we conclude that $\partial(q)\pi=0$.

Put $S=S(\mathfrak{h})$ and $J=I(\mathfrak{h})$ and let J_+ be the ideal in J spanned by all homogeneous elements of J of positive degree. Since W is a finite group generated by reflexions, it follows from a result of Chevalley [2] that the dimension of the vector space S/J_+S is equal to the order w of W. Moreover if Q_S and Q_J are the quotient fields of S and J respectively, then $[Q_S:Q_J]=w$ where $[Q_S:Q_J]$ denotes, as usual, the degree of the field-extension Q_S/Q_J. It is obvious that if an element of S lies in J, the same holds for all its homogeneous components. Hence we can select homogeneous elements $v_1,\cdots,v_w \in S$ such that $S=V+J_+S$, where V is the linear space spanned over C by $(v_1,\cdots,v_w)$.

LEMMA 11. *Every element v of $S(\mathfrak{h})$ can be written exactly in one way in the form $v=u_1v_1+\cdots+u_wv_w$, where $u_i \in I(\mathfrak{h})$ $(1 \leqq i \leqq w)$.*

It follows easily by induction on m that $S=JV+J_+{}^mS$ $(m \geqq 1)$. Let v be any homogeneous element in S of degree d and let d_i be the degree of v_i. Choose $m>d$ and select elements $u_1',\cdots,u_w' \in J$ such that $v-(u_1'v_1+\cdots+u_w'v_w) \in J_+{}^mS$. Let u_i denote the homogeneous component of u_i' of degree $d-d_i$. Then by considering the homogeneous component of of degree d in the above relation, it is clear that $v-(u_1v_1+\cdots+u_wv_w)=0$. This proves that $S=Jv_1+\cdots+Jv_w$ and now it follows easily that $Q_S=Q_JS=\sum_{i=1}^{w} Q_Jv_i$. However $[Q_S:Q_J]=w$ and so $v_1,\cdots,v_w$ must be linearly independent over Q_J. This proves that an element $v \in S$ can be written in exactly one way in the form $v = u_1 v_1 + \cdots + u_w v_w$ $(u_i \in J)$.

We shall now make use of the above lemma to obtain some results on the solutions of a certain system of differential equations which will be important for our applications.

LEMMA 12. *Let* τ *be a distribution on an open subset* U *of* $\mathfrak{h}_0$. *Suppose for each* $q \in I(\mathfrak{h})$, *there exists a complex number* c_q *such that* $\partial(q)\tau = c_q \tau$. *Then* τ *coincides with an analytic function on* U.

Let $H_1, \cdots, H_l$ be a base for $\mathfrak{h}_0$ over R. Put $\Omega = H_1^2 + H_2^2 + \cdots + H_l^2 \in S(\mathfrak{h})$ and consider the polynomial

$$\prod_{s \in W} (\zeta - \Omega^s) = \zeta^w + q_1 \zeta^{w-1} + \cdots + q_w$$

in the indeterminants ζ with coefficients $q_i \in I(\mathfrak{h})$. Then

$$\Omega^w + \Omega^{w-1} q_1 + \cdots + q_w = \prod_{s \in W} (\Omega - \Omega^s) = 0$$

and therefore $\{\partial(\Omega)^w + c_1 \partial(\Omega)^{w-1} + \cdots + c_w\}\tau = 0$, where $c_i = c_{q_i}$ $(1 \leqq i \leqq w)$. However the above differential equation is obviously of the elliptic type (see [3] for the definition of ellipticity). Therefore (see Schwartz [8(I), p. 136] and John [5]), τ is an analytic function on U.

LEMMA 13. *Define* $(v_1, \cdots, v_w)$ *as in Lemma* 11 *and let* ϕ *be an analytic function on a nonempty open connected subset* U *of* $\mathfrak{h}_0$. *Suppose* ϕ *is an eigenfunction of* $\partial(u)$ *for every* $u \in I(\mathfrak{h})$. *Then if* $\partial(v_i)\phi$ $(1 \leqq i \leqq w)$ *all vanish simultaneously at some point of* U, ϕ *must be identically zero.*

Suppose $\phi(H_0; \partial(v_i)) = 0$ $(1 \leqq i \leqq w)$ for some $H_0 \in U$. For any $v \in S(\mathfrak{h})$, we can select $u_1, \cdots, u_w \in I(\mathfrak{h})$ such that $v = \sum_{i=1}^{w} u_i v_i$ (Lemma 11). But then $\partial(u_i)\phi = c_i \phi$ $(c_i \in C)$ and therefore

$$\phi(H_0; \partial(v)) = \sum_{i=1}^{w} c_i \phi(H_0; \partial(v_i)) = 0.$$

This shows that all derivatives of ϕ vanish at H_0 and so ϕ, being an analytic function, must be identically zero.

COROLLARY. *Suppose* H' *is a point in* $\mathfrak{h}$ *such that* $\pi(H') \neq 0$ *and* ϕ *an analytic function on* U *satisfying the system of differential equations*

$$\partial(q)\phi = q(H')\phi \qquad (q \in I(\mathfrak{h})).$$

Then there exist constants c_s $(s \in W)$ *such that*

$$\phi(H) = \sum_{s \in W} c_s \exp B(H, sH') \qquad (H \in U).$$

Moreover they are uniquely determined.

It follows from Lemma 4 of [4(e)] that the w points sH' $(s \in W)$ are all distinct. Put $\phi_s(H) = \exp B(H, sH')$ $(H \in U)$. Then ϕ_s $(s \in W)$ are linearly independent analytic functions on U (see Lemma 41 of [4(b)]). Moreover since $\partial(H)\phi_s = B(H, sH')\phi_s$ $(H \in \mathfrak{h})$, it is clear that $\partial(q)\phi_s = q(H')\phi_s$ for $q \in I(\mathfrak{h})$. Therefore ϕ_s is a solution of our system of differential equations. Let E be the vector space (over C) consisting of all analytic solutions of this system. It is obviously enough to prove that ϕ_s $(s \in W)$ form a base for E or, what is equivalent, that $\dim E \leqq w$. Choose a point $H_0 \in U$. Assuming that $\dim E > w$, we can select $\phi \neq 0$ in E satisfying the w linear conditions $\phi(H_0; \partial(v_i)) = 0$ $1 \leqq i \leqq w$. But we know from Lemma 13 that this is impossible.

The following lemma will be required in another paper.

LEMMA 14. *Suppose ϕ is an analytic function on U such that $\partial(q)\phi = 0$ for all homogeneous elements $q \in I(\mathfrak{h})$ of positive degree. Then there exists a polynomial function $p \in S(\mathfrak{h})$ such that $\phi = p$ on U.*

For any $H \in \mathfrak{h}$, consider the polynomial

$$\prod_{s \in W} (\zeta - sH) = \zeta^w + q_1\zeta^{w-1} + \cdots + q_w$$

in the indeterminants ζ with coefficients $q_i \in I(\mathfrak{h})$. Then $H^w + H^{w-1}q_1 + \cdots + q_w = 0$; and therefore $\partial(H^w + H^{w-1}q_1 + \cdots + q_w)\phi = 0$. But since q_i are all homogeneous and of positive degree, $\partial(q_i)\phi = 0$ $(1 \leqq i \leqq w)$ and therefore $\partial(H^w)\phi = 0$. Hence if $H_1, \cdots, H_l$ is a base for $\mathfrak{h}_0$ over R, $\partial(H_i^w)\phi = 0$ $1 \leqq i \leqq l$. Obviously, this implies that ϕ is a polynomial of degree $\leqq lw$.

5. Applications to the compact case.

In this section we shall assume that G is compact. Let dx denote the normalized Haar measure of G, so that $\int_G dx = 1$. For any $f \in C^\infty(\mathfrak{g}_0)$, let ϕ_f denote the function on $\mathfrak{h}_0$ given by

$$\phi_f(H) = \pi(H) \int_G f(xH)\,dx \qquad (H \in \mathfrak{h}_0).$$

It is obvious that $\phi_f \in C^\infty(\mathfrak{h}_0)$. Define δ as in Theorem 1.

LEMMA 15. *$\phi_{\xi f} = \delta(\xi)\phi_f$ for $\xi \in \mathfrak{J}(\mathfrak{g})$ and $f \in C^\infty(\mathfrak{g}_0)$.*

We use the notation of Section 3. It follows from Lemmas 3 and 5 that we can select elements $s_i \in \mathfrak{S}'$, $h_i \in S(\mathfrak{h})$ and analytic functions a_i $(1 \leqq i \leqq m)$ on $\mathfrak{h}_0'$ such that

$$f(xH;\xi) = f(x:H;\delta'(\xi)) + \sum_{i=1}^{m} a_i(H) f(x;s_i:H;\partial(h_i))$$

for $H \in \mathfrak{h}_0'$. But it is obvious that $\int_G f(x;b:H)dx = 0$ $(H \in \mathfrak{h}_0)$ for $b \in \mathfrak{B}\mathfrak{g}$. Hence it follows from Theorem 1 that

$$\phi_{\xi f}(H) = \pi(H) \int_G f(x:H;\delta'(\xi))dx = \phi_f(H;\delta(\xi)) \qquad (H \in \mathfrak{h}_0').$$

However, $\phi_{\xi f}$ and $\delta(\xi)\phi_f$ are both in $C^\infty(\mathfrak{h}_0)$ and $\mathfrak{h}_0'$ is dense in $\mathfrak{h}_0$. Therefore $\phi_{\xi f} = \delta(\xi)\phi_f$.

Lemma 16. *$\phi_f(0;\delta(\pi)) = \langle \pi, \pi \rangle f(0)$ for all $f \in C^\infty(\mathfrak{g}_0)$.*

Put $g(H) = \int f(xH)dx$ $(H \in \mathfrak{h}_0)$. Since π is a homogeneous polynomial, it is obvious that the local expression of $\partial(\pi) \circ \pi$ at the origin is exactly $\langle \pi, \pi \rangle$. Hence the value of $\partial(\pi)\phi_f$ at zero is $\langle \pi, \pi \rangle g(0) = \langle \pi, \pi \rangle f(0)$.

As usual, we define $\epsilon(s) = 1$ or -1 according as $\pi^s = \pi$ or $-\pi$ $(s \in W)$.

Theorem 2.

$$\pi(H)\pi(H') \int_G \exp B(xH, H')dx = w^{-1}\langle \pi, \pi \rangle \sum_{s \in W} \epsilon(s) \exp B(sH, H')$$

for all $H, H' \in \mathfrak{h}$.

Select an element $H' \in \mathfrak{h}$ such that $\pi(H') \neq 0$, and put $f(X) = \exp B(X, H')$ $(X \in \mathfrak{g}_0)$. Then

$$\phi_f(H) = \pi(H) \int_G \exp B(xH, H')dx$$

and therefore, from Theorem 1 and Lemma 15, $\phi_{\partial(p)f} = \partial(\bar{p})\phi_f$ $(p \in I(\mathfrak{g})$. But it is clear that $\partial(Y)f = B(Y, H')f$ $(Y \in \mathfrak{g})$, and so $\partial(q) = q(H')f$ for $q \in S(\mathfrak{g})$. Hence $\partial(\bar{p})\phi_f = p(H')\phi_f$ $(p \in I(\mathfrak{g}))$. But in view of Lemma 9, this implies that $\partial(q)\phi_f = q(H')\phi_f$ for all $q \in I(\mathfrak{h})$, and we conclude from the Corollary to Lemma 13 that

$$\phi_f(H) = \sum_{s \in W} c_s \exp B(sH, H') \qquad (H \in \mathfrak{h}_0),$$

where c_s $(s \in W)$ are constants. On the other hand, since G is compact, we can select, for each $s \in W$, an element $x_s \in G$ such that $x_s H = sH$ $(H \in \mathfrak{h}_0)$.

Therefore it is obvious that s maps $\mathfrak{h}_0$ into itself and $\phi_f(sH) = \epsilon(s)\phi_f(H)$, and so

$$\phi_f(H) = w^{-1} \sum_{s \in W} \epsilon(s)\phi_f(sH) = w^{-1}c \sum_{s \in W} \epsilon(s) \exp B(sH, H') \qquad (H \in \mathfrak{h}_0),$$

where $c = \sum_{s \in W} \epsilon(s) c_s$. On the other hand, $\phi_f(0\,;\partial(\pi)) = \langle\pi,\pi\rangle f(0) = \langle\pi,\pi\rangle$ from Lemma 16. Put $\psi_s(H) = \exp B(sH, H')$ $(H \in \mathfrak{h}_0)$. Then $\partial(q)\psi_s = q(s^{-1}H')\psi_s$ $(q \in S(\mathfrak{h}))$, and therefore $\partial(\pi)\psi_s = \epsilon(s)\pi(H')\psi_s$. Hence

$$\langle\pi,\pi\rangle = \phi_f(0\,;\partial(\pi)) = w^{-1}c\pi(H')w = c\pi(H'),$$

and so $c = \langle\pi,\pi\rangle/\pi(H')$. This proves that

$$\pi(H)\pi(H') \int_G \exp B(x, H, H')dx = w^{-1}\langle\pi,\pi\rangle \sum_{s \in W} \epsilon(s) \exp B(sH, H')$$

for $H \in \mathfrak{h}_0$ and $H' \in \mathfrak{h}$ provided $\pi(H') \neq 0$. But since both sides can obviously be considered as holomorphic functions on $\mathfrak{h} \times \mathfrak{h}$, it follows that they must be equal for all $H, H' \in \mathfrak{h}$.

Let dX and dH denote the Euclidean measures on $\mathfrak{g}_0$ and $\mathfrak{h}_0$, respectively. We may assume (see Lemma 9 of [4(d)]) that they are so normalized that

$$\int_{\mathfrak{g}_0} f(X)\,dX = \int_{\mathfrak{h}_0} |\pi(H)|^2\, dH \int_G f(xH)\,dx \qquad (f \in C_c(\mathfrak{g}))$$

For any $f \in \mathscr{C}(\mathfrak{g}_0)$ and $g \in \mathscr{C}(\mathfrak{h}_0)$, let $\bar{f}$ and $\tilde{g}$ denote the corresponding Fourier transforms, so that

$$\bar{f}(Y) = \int_{\mathfrak{g}_0} \exp\{(-1)^{\frac{1}{2}}B(Y,X)\}f(X)dX,$$

$$\tilde{g}(H') = \int_{\mathfrak{h}_0} \exp\{(-1)^{\frac{1}{2}}B(H',H)\}g(H)dH$$

$(Y \in \mathfrak{g}_0, H' \in \mathfrak{h}_0)$. Then we have the following result.

THEOREM 3. *If $f \in \mathscr{C}(\mathfrak{g}_0)$, the corresponding function ϕ_f lies in $\mathscr{C}(\mathfrak{h}_0)$ and $f \to \phi_f$ is a continuous mapping of $\mathscr{C}(\mathfrak{g}_0)$ into $\mathscr{C}(\mathfrak{h}_0)$. Moreover*[3] $\phi_{\bar{f}} = (-1)^r\langle\pi,\pi\rangle(\phi_f)^{\sim}$, *where r is the number of positive roots.*

It is seen without difficulty that for any $D \in \mathfrak{D}(\mathfrak{g})$, we can find a finite number of elements $D_1, \cdots, D_m \in \mathfrak{D}(\mathfrak{g})$ and analytic functions $a_1, \cdots, a_m$ on G such that $D^x = a_1(x)D_1 + \cdots + a_m(x)D_m$ $(x \in G)$. Now suppose $f \in \mathscr{C}(\mathfrak{g}_0)$ and $d \in \mathfrak{D}(\mathfrak{h})$. Then it is clear that

$$\phi_f(H\,;d) = \int_G f(xH\,;D^x)\,dx \qquad (H \in \mathfrak{h}_0)$$

where $D = d \circ \pi$. Since G is compact, we can select a positive number c such that $|a_i(x)| \leqq c$ $(1 \leqq i \leqq m, x \in G)$. Hence

$$|\phi_f(H;d)| \leqq \sum_{i=1}^{m} c \sup_{X \in \mathfrak{g}_0} |f(X;D_i)|,$$

and this proves that $\phi_f \in \mathscr{C}(\mathfrak{h}_0)$ and the mapping $f \rightarrow \phi_f$ of $\mathscr{C}(\mathfrak{g}_0)$ into $\mathscr{C}(\mathfrak{h}_0)$ is continuous.

Put $\eta(X:Y) = \exp\{(-1)^{\frac{1}{2}} B(X,Y)\}$ $(X, Y \in \mathfrak{g}_0)$. Then if $f \in \mathscr{C}(\mathfrak{g}_0)$,

$$\phi_{\tilde{f}}(H) = \pi(H) \int_G \tilde{f}(xH)dx = \pi(H) \int_G dx \int_{\mathfrak{g}_0} \eta(xH:Y)f(Y)dY \quad (H \in \mathfrak{h}_0).$$

But

$$\int_{\mathfrak{g}_0} \eta(xH:Y)f(Y)dY = \int_{G \times \mathfrak{h}_0} \eta(xH:yH') \,|\pi(H')|^2 f(yH')dy\,dH'$$

$$= (-1)^r \int_{G \times \mathfrak{h}_0} \eta(xH:yH')\pi(H')^2 f(yH')dy\,dH'$$

since every root takes only pure imaginary values on $\mathfrak{h}_0$. Therefore we conclude from Theorem 2 that

$$\phi_{\tilde{f}}(H) = w^{-1}\langle\pi,\pi\rangle(-1)^r \sum_{s \in W} \epsilon(s) \int_{G \times \mathfrak{h}_0} \pi(H')\eta(sH:H')f(yH')dy\,dH'$$

$$= (-1)^r w^{-1}\langle\pi,\pi\rangle \sum_{s \in W} \epsilon(s) \int_{\mathfrak{h}_0} \eta(sH:H')\phi_f(H')dH'.$$

But we have seen that $\phi_f(sH') = \epsilon(s)\phi_f(H')$ $(s \in W)$. Hence

$$\int_{\mathfrak{h}_0} \eta(sH:H')\phi_f(H')dH' = \int_{\mathfrak{h}_0} \eta(H:H')\phi_f(sH')dH'$$

$$= \epsilon(s) \int_{\mathfrak{h}_0} \eta(H:H')\phi_f(H')dH'.$$

This proves that $\phi_{\tilde{f}}(H) = (-1)^r\langle\pi,\pi\rangle \int \eta(H:H')\phi_f(H')dH'$ $(H \in \mathfrak{h}_0)$, and therefore $\phi_{\tilde{f}} = (-1)^r\langle\pi,\pi\rangle(\phi_f)^{\sim}$.

In another paper we shall obtain a suitable analogue of the above theorem for the case when G is not compact.

Let $J(\mathfrak{g}_0)$ and $J(\mathfrak{h}_0)$ denote the sets of all functions in $\mathscr{C}(\mathfrak{g}_0)$ and $\mathscr{C}(\mathfrak{h}_0)$ which are invariant under G and W respectively. For any function f on $\mathfrak{g}_0$, let $\bar{f}$ denote its restriction on $\mathfrak{h}_0$.

THEOREM 4. *If* $f \in J(\mathfrak{g}_0)$, *then* $\bar{f} \in J(\mathfrak{h}_0)$ *and* $f \rightarrow \bar{f}$ *is a topological mapping of* $J(\mathfrak{g}_0)$ *onto* $J(\mathfrak{h}_0)$.

Put $\eta'(X:Y) = \exp\{-(-1)^{\frac{1}{2}}B(X,Y)\}$ $(X, Y \in \mathfrak{g}_0)$. Then if $p \in S(\mathfrak{g})$, it is clear that $\eta'(X;\partial(p):Y) = \hat{p}(Y)\eta'(X:Y)$ where $\hat{p}$ is the polynomial function $Z \to p(-(-1)^{\frac{1}{2}}Z)$ on $\mathfrak{g}$. Now we assume that the normalization of the Euclidean measure dH on $\mathfrak{h}_0$ is regular and put

$$\psi_g(X) = \int_{\mathfrak{h}_0} \xi(X:H)\pi(H)\tilde{g}(H;\partial(\pi))dH \qquad (g \in J(\mathfrak{h}_0), X \in \mathfrak{g}_0),$$

where $\xi(X:Y) = \int_G \eta'(xX:Y)dx$ $(X, Y \in \mathfrak{g}_0)$. Then it follows from Theorem 2 that if $H' \in \mathfrak{h}_0$,

$$\pi(H')\psi_g(H') = c \int_{\mathfrak{h}_0} \sum_{s \in W} \epsilon(s)\eta'(H:sH')\tilde{g}(H;\partial(\pi))dH,$$

where $c = w^{-1}\langle\pi,\pi\rangle$. Now it is clear that[11]

$$\int_{\mathfrak{h}_0} \eta'(H:sH')\tilde{g}(H;\partial(\pi))dH = (-1)^r \int_{\mathfrak{h}_0} \eta'(H;\partial(\pi):sH')\tilde{g}(H)dH$$
$$= (-1)^r\hat{\pi}(sH') \int \eta'(H:sH')\tilde{g}(H)dH = (-1)^{r/2}\epsilon(s)\pi(H')g(sH')$$

$(s \in W)$. Therefore, since g is invariant under W, we get

$$\pi(H')\psi_g(H') = (-1)^{r/2}\, wc\pi(H')g(H') \qquad (H' \in \mathfrak{h}_0).$$

But as $\bar{\psi}_g$ and g are both of class C^∞, this implies that $\bar{\psi}_g = c'g$, where $c' = (-1)^{r/2}\langle\pi,\pi\rangle$. It is obvious from its definition that $\psi_g \in C^\infty(\mathfrak{g}_0)$ and it is invariant under G. Moreover, since $\mathfrak{g}_0 = \bigcup_{x \in G} x\mathfrak{h}_0$, it is obvious that ψ_g is the only invariant function on $\mathfrak{g}_0$ which coincides with $c'g$ on $\mathfrak{h}$. Therefore $q\psi_g = \psi_{\bar{q}g}$ if $q \in I(\mathfrak{g})$.

Put

$$\nu_D(F) = \sup_{X \in \mathfrak{g}_0} |F(X;D)|, \qquad \sigma_d(\phi) = \sup_{H \in \mathfrak{h}_0} |\phi(H;d)|$$

for $F \in C^\infty(\mathfrak{g}_0)$, $\phi \in C^\infty(\mathfrak{h})$, $D \in \mathfrak{D}(\mathfrak{g})$ and $d \in \mathfrak{D}(\mathfrak{h})$. We claim that for any $D \in \mathfrak{D}(\mathfrak{g})$, we can select a finite number of elements $d_1, \cdots, d_N \in \mathfrak{D}(\mathfrak{h})$ such that

$$\nu_D(\psi_g) \leqq \sum_{i=1}^{N} \sigma_{d_i}(g)$$

for $g \in J(\mathfrak{h}_0)$. It is enough to prove this for $D = p\partial(q)$ $(p, q \in S(\mathfrak{g}))$. We shall use induction on the degree of q which we denote by m. If $m = 0$, we may assume that $D = p$. Since G is compact, the Casimir polynomial ω is a negative-definite quadratic form on $\mathfrak{g}_0$, and so it is clear that we can select $p_0 \in I(\mathfrak{g})$ such that p_0 takes only real nonnegative values on $\mathfrak{g}_0$ and $|p(X)| \leqq p_0(X)$ $(X \in \mathfrak{g}_0)$. Then $p_0\psi_g = \psi_{\bar{p}_0 g}$, and therefore $\nu_D(\psi_g) \leqq \nu_{p_0}(\psi_g) = \nu_1(\psi_{\bar{p}_0 g})$. From Lemma 1 and its Corollary, there exist elements $p_1 \in S(\mathfrak{h})$ and $d \in \mathfrak{D}(\mathfrak{h})$ such that $(\bar{p}_0\phi)^{\sim} = \partial(p_1)\bar{\phi}$ and

---

[11] $(-1)^{k/2} = ((-1)^{\frac{1}{2}})^k$ for any integer k.

$$\int_{\mathfrak{h}_0} |\pi\partial(\pi p_1)\bar{\phi}|\, dH \leqq \sigma_d(\phi)$$

for $\phi \in \mathscr{B}(\mathfrak{h}_0)$. Therefore

$$\nu_D(\psi_g) \leqq \nu_1(\psi_{\bar{p}_0 g}) \leqq \int |\pi\partial(\pi p_1)\bar{g}|\, dH \leqq \sigma_d(g) \qquad (g \in J(\mathfrak{h}_0))$$

since $|\xi(X:Y)| \leqq 1$ $(X, Y \in \mathfrak{g}_0)$. Now suppose $m \geqq 1$. Again choose $p_0 \in I(\mathfrak{g})$ such that $|p(X)| \leqq p_0(X)$ for $X \in \mathfrak{g}_0$. Then if $D_0 = p_0\partial(q)$, it is obvious that $\nu_D(\psi_g) \leqq \nu_{D_0}(\psi_g)$. Also, it is clear that

$$D_0 = \partial(q) \circ p_0 + \sum_{i=1}^{k} p_i\partial(q_i),$$

where k is some integer, $p_i, q_i \in S(\mathfrak{g})$ and the degree of each q_i is smaller than m. In view of the induction hypothesis, it is sufficient to prove our statement for $\Delta = \partial(q) \circ p_0$. But $\Delta\psi_g = \partial(q)\psi_{g_0}$, where $g_0 = \bar{p}_0 g$, and

$$\xi(X;\partial(q):Y) = \int_G \hat{q}(xY)\eta'(X:xY)\,dx \qquad (X, Y \in \mathfrak{g}_0).$$

We again select $q_0 \in I(\mathfrak{g})$ such that $|\hat{q}(X)| \leqq q_0(X)$ for $X \in \mathfrak{g}_0$. Then $|\xi(X;\partial(q):Y)| \leqq q_0(Y)$ $(X, Y \in \mathfrak{g}_0)$, and therefore

$$|\psi_{g_0}(X;\partial(q))| \leqq \int_{\mathfrak{h}_0} |\bar{q}_0\pi\partial(\pi)\bar{g}_0|\, dH.$$

Choose $p_1 \in S(\mathfrak{h})$ and $d \in \mathfrak{D}(\mathfrak{h})$ such that $(\bar{p}_0\phi)^{\sim} = \partial(p_1)\bar{\phi}$ and

$$\int_{\mathfrak{h}_0} |\bar{q}_0\pi\partial(\pi p_1)\bar{\phi}|\, dH \leqq \sigma_d(\phi)$$

for $\phi \in \mathscr{B}(\mathfrak{h})$. Then $\nu_\Delta(\psi_g) = \nu_{\partial(q)}(\psi_{g_0}) \leqq \sigma_d(g)$ $(g \in J(\mathfrak{h}_0))$.

The above result shows that if $g \in J(\mathfrak{h}_0)$, then ψ_g lies in $J(\mathfrak{g}_0)$ and[12] $\psi' : g \to (c')^{-1}\psi_g$ is a continuous mapping of $J(\mathfrak{h}_0)$ into $J(\mathfrak{g}_0)$. On the other hand, it is obvious that if $f \in J(\mathfrak{g}_0)$, then $\bar{f} \in J(\mathfrak{h}_0)$ and the mapping $\tau : f \to \bar{f}$ of $J(\mathfrak{g}_0)$ into $J(\mathfrak{h}_0)$ is continuous and univalent. Since $\tau(\psi_g) = c'g$, it follows that $\psi_{\bar{f}} = c'f$ and therefore these two mappings τ and ψ' are inverses of each other. Hence the theorem.

The following result will be needed in Section 8.

---

[12] We shall prove in Section 6 that $\langle \pi, \pi \rangle \neq 0$ (see the Corollary to Lemma 18).

LEMMA 17. *For any* $f \in \mathscr{C}(\mathfrak{h}_0)$ *there exists a unique element* Ψ_f *in* $J(\mathfrak{h}_0)$ *such that*

$$\pi(H)\Psi_f(H) = \sum_{s \in W} \epsilon(s) f(sH) \qquad (H \in \mathfrak{h}_0).$$

Moreover $f \to \Psi_f$ *is a continuous mapping of* $\mathscr{C}(\mathfrak{h}_0)$ *into* $J(\mathfrak{g}_0)$.

Put

$$\Psi_f(X) = c_1 \int_{\mathfrak{h}_0} \xi(X:H)\pi(H) \sum_{s \in W} \epsilon(s)\bar{f}(sH)\,dH \qquad (f \in \mathscr{C}(\mathfrak{h}_0), X \in \mathfrak{g}_0),$$

where $\bar{f}$ is the Fourier transform of f and[12] $c_1 = \langle \pi, \pi \rangle^{-1}$. Then it follows from Theorem 2 that

$$\pi(H')\Psi_f(H') = \sum_{s \in W} \epsilon(s) f(sH') \qquad (H' \in \mathfrak{h}_0).$$

Furthermore, we show exactly as above that $\Psi_f \in J(\mathfrak{g}_0)$ and the mapping $f \to \Psi_f$ is continuous. Finally, since $\mathfrak{g}_0 = \bigcup_{x \in G} x\mathfrak{h}_0$, every invariant function in $C^\infty(\mathfrak{g}_0)$ is uniquely determined by its restriction on $\mathfrak{g}_0'$. This proves the uniqueness of Ψ_f.

6. Some further results. We now discard the assumption about the compactness of G. Define δ as in Theorem 1, and, for $\xi \in \mathfrak{D}(\mathfrak{g})$ and $\eta \in \mathfrak{D}(\mathfrak{h})$, let ξ_0 and η_0 denote their respective local expressions at zero. It is clear that if $\xi \in \mathfrak{I}(\mathfrak{g})$, then $\xi_0 \in \partial(I(\mathfrak{g}))$.

LEMMA 18. $(\partial(\pi) \circ \delta(\xi))_0 = (\partial(\pi) \circ \delta(\xi_0))_0$ *for every* $\xi \in \mathfrak{I}(\mathfrak{g})$.

It is known (see Mostow [7]) that we can find a compact real form $\mathfrak{u}$ of $\mathfrak{g}$ such that $\mathfrak{h} \cap \mathfrak{u}$ is a Cartan subalgebra of $\mathfrak{u}$. Let G_c be the (connected) complex adjoint group of $\mathfrak{g}$ and U the (connected) adjoint group of $\mathfrak{u}$. Then both G and U are real analytic subgroups of G_c corresponding to the real subalgebras $\mathfrak{g}_0$ and $\mathfrak{u}$ of $\mathfrak{g}$. Then (see Section 2) G_c operates on $\mathfrak{D}(\mathfrak{g})$, and it is clear that $I(\mathfrak{g})$ is exactly the algebra of those polynomials p on $\mathfrak{g}$ which are invariant under G_c. Therefore the two algebras $\mathfrak{I}(\mathfrak{g})$ and $\mathfrak{I}(\mathfrak{h})$ are the same whether we start from the real form $\mathfrak{g}_0$ or $\mathfrak{u}$. Let du denote the normalized Haar measure of U, and for any $f \in C^\infty(\mathfrak{u})$ define

$$\phi_f(H) = \pi(H) \int_U f(uH)\,du \qquad (H \in \mathfrak{h} \cap \mathfrak{u})$$

as in Section 5. In order to prove the lemma, let us first suppose that $\xi_0 = 0$. Then from Lemma 16, $\phi_{\xi f}(0; \partial(\pi)) = 0$ for all $f \in C^\infty(\mathfrak{u})$. But we know (Lemma 15) that $\phi_{\xi f} = \delta(\xi)\phi_f$. This proves that $\partial(\pi)(\delta(\xi)\phi_f)$ has the value zero at the origin. Now suppose $f \in I(\mathfrak{g})$. Then $\phi_f = \pi\bar{f}$, where $\bar{f}$ is the restriction of f on $\mathfrak{h} \cap \mathfrak{u}$. Hence we conclude from Lemma 9 that $(\partial(\pi) \circ \delta(\xi))(\pi p)$ takes the value zero at the origin for every $p \in I(\mathfrak{h})$. Select $q \in S(\mathfrak{h})$ such that $(\partial(\pi) \circ \delta(\xi))_0 = \partial(q)$. Since $\delta(\xi)$ is invariant under W, it is obvious that $q^s = \epsilon(s) q$ $(s \in W)$. We claim $q = 0$. For otherwise we could select $p_1 \in S(\mathfrak{h})$ such that $\langle q, p_1 \rangle \neq 0$. But $\langle q, p_1 \rangle = \langle q^s, p_1{}^s \rangle = \epsilon(s) \langle q, p_1{}^s \rangle$ $(s \in W)$. Hence $\langle q, p_2 \rangle = \langle q, p_1 \rangle \neq 0$, where $p_2 = w^{-1} \sum_{s \in W} \epsilon(s) p_1{}^s$. However it follows from Lemma 10 that $p_2 = \pi p$ for some $p \in I(\mathfrak{h})$, and therefore $\langle q, \pi p \rangle \neq 0$. On the other hand, in view of the definition of q, $\langle q, \pi p \rangle$ is exactly the value of $(\partial(\pi) \circ \delta(\xi))(\pi p)$ at the origin, which, as we have seen above, must be zero. This contradiction proves that $q = 0$, and therefore $(\delta(\pi) \circ \delta(\xi))_0 = 0$. The general case is reduced to the one discussed above by replacing ξ by $\xi - \xi_0$.

Let $\tilde{\theta}$ denote the conjugation of $\mathfrak{g}$ with respect to $\mathfrak{u}$, and $p \rightarrow p_*$ $(p \in S(\mathfrak{g}))$ the automorphism of $S(\mathfrak{g})$ over R which coincides with $-\tilde{\theta}$ on $\mathfrak{g}$. Select a base $X_1, \cdots, X_n$ for $\mathfrak{u}$ over R such that $B(X_i, X_j) = -\delta_{ij}$, $1 \leqq i, j \leqq n$. Then if

$$p = \sum_{m_i \geqq 0} a(m_1, \cdots, m_n) X_1{}^{m_1} \cdots X_n{}^{m_n} \qquad (a(m_1, \cdots, m_n) \in C),$$

it is clear that $\langle p_*, p \rangle = \sum_{m_i \geqq 0} m_1! \cdots m_n! \, | a(m_1, \cdots, m_n) |^2 > 0$ unless $p = 0$. On the other hand, since every root α takes only pure imaginary values on $\mathfrak{h} \cap \mathfrak{u}$, it is obvious that $\pi_* = \pi$. Therefore $\langle \pi^k, \pi^k \rangle$ is a positive real number for every integer $k \geqq 0$. Moreover, since $\pi^2 \in I(\mathfrak{h})$, there exists (Lemma 9) a unique element $\eta \in I(\mathfrak{g})$ such that $\bar{\eta} = \pi^2$. It is clear that η_* is also in $I(\mathfrak{g})$ and $\bar{\eta}_* = (\pi^2)_* = \pi^2 = \bar{\eta}$. Hence we conclude from Lemma 9 that $\eta_* = \eta$, and therefore $\langle \eta^k, \eta^k \rangle > 0$ for any integer $k \geqq 0$. Put $\xi = \partial(\eta^k) \circ \eta^k$ for some fixed k. It is obvious that $\xi_0 = \langle \eta^k, \eta^k \rangle$, and therefore we get the following Corollary from Lemma 18.

COROLLARY. *Put* $\xi = \partial(\eta^k) \circ \eta^k$ *for some integer* $k \geqq 0$. *Then*

$$(\partial(\pi) \circ \delta(\xi))_0 = \langle \eta^k, \eta^k \rangle \partial(\pi).$$

Moreover, $\langle \eta^k, \eta^k \rangle$ *and* $\langle \eta^k, \eta^k \rangle$ *are positive real numbers.*

We shall now prove an algebraic result which will be needed in another paper. As before let ω denote the Casimir polynomial of $\mathfrak{g}$ and define a differential operator σ on $\mathfrak{g}_0$ as follows: $f(X; \sigma) = f(X; \partial(X))$ $(X \in \mathfrak{g}_0$, $f \in C^\infty(\mathfrak{g}_0))$. It is obvious that $\sigma \in \mathfrak{D}(\mathfrak{g})$.

LEMMA 19. *For any integer* $k \geqq 1$,

$$\partial(\omega^k)\circ\omega^k \equiv 4^k k!(\tfrac{1}{2}n+\sigma+k-1)(\tfrac{1}{2}n+\sigma+k-2)\cdots(\tfrac{1}{2}n+\sigma) \mod \omega\mathfrak{D}(\mathfrak{g}),$$

where $n = \dim_C \mathfrak{g}$.

Define $\{D_1, D_2\} = D_1D_2 - D_2D_1$ as before for any two differential operators D_1, D_2. Then a simple calculation shows that $\{\partial(\omega), \omega\} = 2n + 4\sigma$. Moreover, if p is a homogeneous polynomial in $S(\mathfrak{g})$ of degree m, it is easily seen that $\sigma p = mp$, and therefore it is clear that $\partial(\omega)\sigma = (\sigma+2)\partial(\omega)$. Hence

$$\begin{aligned}\{\partial(\omega^k), \omega\} &= \sum_{0\leqq m<k} \partial(\omega^{k-1-m})(2n+4\sigma)\partial(\omega^m)\\ &= \sum_{0\leqq m<k}(2n+4(\sigma+2k-2-2m))\partial(\omega^{k-1})\\ &= 4k(\tfrac{1}{2}n+\sigma+k-1)\partial(\omega^{k-1}).\end{aligned}$$

Therefore

$$\partial(\omega^k)\circ\omega^k \equiv \{\partial(\omega^k),\omega\}\circ\omega^{k-1} \equiv 4k(\tfrac{1}{2}n+\sigma+k-1)\partial(\omega^{k-1})\circ\omega^{k-1} \mod \omega\mathfrak{D}(\mathfrak{g}),$$

and our assertion now follows by induction.

This lemma has the following significance for our later applications. Let t denote a real variable.

COROLLARY. *For any* $f \in C_c^\infty(\mathfrak{g}_0)$, *put* $f_k = \partial(\omega^k)(\omega^k f)$ $(k \geqq 0)$. *Then if* $X \neq 0$ *is an element in* $\mathfrak{g}_0$ *such that* $\omega(X) = 0$, *we have*[13]

$$\int_0^\infty f_k(tX)dt = 4^k k!\{\Gamma(\tfrac{1}{2}n+k-1)/\Gamma(\tfrac{1}{2}n-1)\}\int_0^\infty f(tX)dt$$

for all integers $k \geqq 0$.

It is obvious that $g(tX;\sigma) = tg(tX;\partial(X)) = t(d/dt)g(tX)$ for any $g \in C_c^\infty(\mathfrak{g}_0)$. Hence

$$\int_0^\infty g(tX;\sigma+1)dt = \int_0^\infty (d/dt)(tg(tX))dt = 0.$$

On the other hand, it follows from Lemma 19 that

$$f_k = c_k f + (\sigma+1)g_1 + \omega g_2,$$

where $g_1, g_2 \in C_c^\infty(\mathfrak{g})$ and $c_k = 4^k k!\,\Gamma(\tfrac{1}{2}n+k-1)/\Gamma(\tfrac{1}{2}n-1)$. Therefore, since $\omega(tX) = t^2\omega(X) = 0$, we conclude that

$$\int_0^\infty f_k(tX)dt = c_k\int_0^\infty f(tX)dt.$$

---

[13] Here Γ stands for the classical Gamma function.

7. Differential operators on a reductive subalgebra. Let $\mathfrak{m}_0$ be a Lie subalgebra of $\mathfrak{g}_0$. We assume that $\mathfrak{m}_0 \supset \mathfrak{h}_0$ and $\mathfrak{m}_0$ is reductive in $\mathfrak{g}_0$ (see Koszul [6]). Then we can select a subspace $\mathfrak{q}_0$ of $\mathfrak{g}_0$ such that $[\mathfrak{m}_0, \mathfrak{q}_0] \subset \mathfrak{q}_0$ and $\mathfrak{g}_0$ is the direct sum of $\mathfrak{m}_0$ and $\mathfrak{q}_0$. Let $\mathfrak{m}, \mathfrak{q}$ be the complexification of $\mathfrak{m}_0, \mathfrak{q}_0$, respectively, in $\mathfrak{g}$ and let Q be the set of all roots $\alpha \in P$ for which $X_\alpha \in \mathfrak{m}$. Then it is clear that $\mathfrak{m} = \mathfrak{h} + \sum_{\alpha \in Q} (CX_\alpha + CX_{-\alpha})$ and $\mathfrak{q} = \sum_{\alpha \in Q'} (CX_\alpha + CX_{-\alpha})$, where Q' is the complement of Q in P. Since the restriction of the bilinear form B on $\mathfrak{m}$ is obviously nondegenerate, we can apply the formalism described in Section 2 to $E_0 = \mathfrak{g}_0$ and $F_0 = \mathfrak{m}_0$. For any $X \in \mathfrak{m}$, let $\zeta(X)$ denote the determinant of the restriction of $\operatorname{ad} X$ on $\mathfrak{q}$. (If $\mathfrak{q} = \{0\}$, we define $\zeta(X)$ to be 1.) Then ζ, being a polynomial function on $\mathfrak{m}$, lies in $S(\mathfrak{m})$. Moreover, ζ coincides on $\mathfrak{h}$ with $(-1)^s \prod_{\alpha \in Q'} \alpha^2$, where s is the number of roots in Q'. Hence $\zeta \neq 0$. Let $\mathfrak{m}_0'$ denote the set of all $X \in \mathfrak{m}_0$ where $\zeta(X) \neq 0$. Then $\mathfrak{m}_0'$ is an open dense subset of $\mathfrak{m}_0$ and $\mathfrak{h}_0' \subset \mathfrak{m}_0'$. Put $\mathfrak{Q} = \lambda(S(\mathfrak{q}))$, where λ is the canonical mapping of $S(\mathfrak{g})$ into $\mathfrak{B}$. The next two lemmas are proved in the same way as Lemmas 4 and 5.

LEMMA 20. *If $X \in \mathfrak{m}_0'$, Γ_X defines a one-one mapping of $\mathfrak{Q} \times S(\mathfrak{m})$ onto $S(\mathfrak{g})$.*

LEMMA 21. *For every $p \in S(\mathfrak{g})$, there exists an integer $k \geqq 0$ and a polynomial mapping γ_p of $\mathfrak{m}$ into $\mathfrak{Q} \times S(\mathfrak{m})$ such that $\Gamma_X(\gamma_p(X)) = \zeta(X)^k p$ $(X \in \mathfrak{m}_0)$.*

For any $x \in G$, let $b \to b^x$ $(b \in \mathfrak{B})$ denote the unique automorphism of $\mathfrak{B}$ which coincides with x on $\mathfrak{g}$. Then we also get an automorphism $\mu \to \mu^x$ of $\mathfrak{B} \times S(\mathfrak{g})$ given by $(b \times p)^x = b^x \times p^x$ $(b \in \mathfrak{B}, p \in S(\mathfrak{g}))$. It is obvious from the definition of Γ_Y $(Y \in \mathfrak{g}_0)$ that $(\Gamma_Y(\mu))^x = \Gamma_{xY}(\mu^x)$ $(\mu \in \mathfrak{B} \times S(\mathfrak{g}))$. Let M be the analytic subgroup of G corresponding to $\mathfrak{m}_0$. It is obvious that $\zeta^m = \zeta$, and therefore $m\mathfrak{m}_0' = \mathfrak{m}_0'$ $(m \in M)$. For any $p \in S(\mathfrak{g})$, let $\beta_p(X)$ $(X \in \mathfrak{m}_0')$ denote the unique element in $\mathfrak{Q} \times S(\mathfrak{m})$ (see Lemma 20) such that $\Gamma_X(\beta_p(X)) = p$. Then if $m \in M$,

$$p^m = (\Gamma_X(\beta_p(X)))^m = \Gamma_{mX}(\beta_p(X)^m) \qquad (X \in \mathfrak{m}_0'),$$

and this shows that $\beta_{p^m}(mX) = (\beta_p(X))^m$. Thus we have obtained the following result.

LEMMA 22. *For any $p \in S(\mathfrak{g})$ and $X \in \mathfrak{m}_0'$, let β_p denote the unique* *element in* $\mathfrak{Q}\times S(\mathfrak{m})$ *such that* $\Gamma_X(\beta_p(X))=p$. *Then* $\beta_{p^m}(mX)=(\beta_p(X))^m$ $(m\in M)$.

Put $\mathfrak{Q}'=\sum_{d\geqq 1}\lambda(S_d(\mathfrak{q}))$, where $S_d(\mathfrak{q})$ is the space of homogeneous elements in $S(\mathfrak{q})$ of degree d. Let $\mu_X(p)$ $(X\in\mathfrak{m}_0', p\in S(\mathfrak{g}))$ denote the unique element in $S(\mathfrak{m})$ such that $\beta_p(X)-(1\times\mu_X(p))\in\mathfrak{Q}'\times S(\mathfrak{m})$. Then it follows from Lemma 21 that there exists a differential operator $\Delta(p)$ on $\mathfrak{m}_0'$ whose local expression at X coincides with $\partial(\mu_X(p))$. On the other hand, since ζ is nowhere zero on $\mathfrak{m}_0'$, $|\zeta|^{\frac{1}{2}}$ and $|\zeta|^{-\frac{1}{2}}$ are analytic functions on $\mathfrak{m}_0'$, and so, for any $q\in S(\mathfrak{m})$, $|\zeta|^{-\frac{1}{2}}\partial(q)\circ|\zeta|^{\frac{1}{2}}$ is a well-defined differential operator on $\mathfrak{m}_0'$. Let $p_\mathfrak{m}$ denote the restriction of a polynomial $p\in S(\mathfrak{g})$ on $\mathfrak{m}$. Then $p_\mathfrak{m}\in S(\mathfrak{m})$ and $\Delta(p)-|\zeta|^{-\frac{1}{2}}\partial(p_\mathfrak{m})\circ|\zeta|^{\frac{1}{2}}$ is a differential operator on $\mathfrak{m}_0'$. We shall denote its local expression at $X\in\mathfrak{m}_0'$ in the usual way by $(\Delta(p)-|\zeta|^{-\frac{1}{2}}\partial(p_\mathfrak{m})\circ|\zeta|^{\frac{1}{2}})_X$. Let $\mathfrak{M}$ be the subalgebra of $\mathfrak{B}$ generated by $(1,\mathfrak{m})$. We put $\mathfrak{M}'=\mathfrak{M}\mathfrak{m}$.

LEMMA 23. *If* $p\in I(\mathfrak{g})$ *and* $X\in\bigcup_{m\in M}m\mathfrak{h}_0'$, *then*

$$(\Delta(p)-|\zeta|^{-\frac{1}{2}}\partial(p_\mathfrak{m})\circ|\zeta|^{\frac{1}{2}})_X\in\partial(\Gamma_X(\mathfrak{M}'\times S(\mathfrak{m}))).$$

Let $D=\Delta(p)-|\zeta|^{-\frac{1}{2}}\partial(p_\mathfrak{m})\circ|\zeta|^{\frac{1}{2}}$. Since both ζ and $p_\mathfrak{m}$ are invariant under M, it follows from Lemma 22 that $D_{mX}=(D_X)^m$ $(m\in M, X\in\mathfrak{m}_0')$. Hence it would be sufficient to prove that D_H lies in $\partial(\Gamma_H(\mathfrak{M}'\times S(\mathfrak{m})))$ for $H\in\mathfrak{h}_0'$. Since $\mathfrak{m}_0$ is reductive, it is clear that Lemma 4 can be applied to $\mathfrak{m}_0$ in place of $\mathfrak{g}_0$. We now use the notation of Section 3 and put $\mathfrak{S}_\mathfrak{m}=\mathfrak{S}\cap\mathfrak{M}$ and $\mathfrak{S}_\mathfrak{m}'=\mathfrak{S}'\cap\mathfrak{M}$. Also fix an element $H_0\in\mathfrak{h}_0'$. Since $S(\mathfrak{s})\cap S(\mathfrak{m})=S(\mathfrak{s}\cap\mathfrak{m})$ and the canonical mapping λ of $S(\mathfrak{g})$ onto $\mathfrak{B}$ is a linear isomorphism, it follows that $\lambda(S(\mathfrak{s}\cap\mathfrak{m}))=\mathfrak{S}_\mathfrak{m}$ and $\mathfrak{S}_\mathfrak{m}'=\mathfrak{S}\cap\mathfrak{M}'$. Therefore from Lemma 4 (applied to $\mathfrak{m}_0$), Γ_{H_0} defines a one-one mapping of $\mathfrak{S}_\mathfrak{m}\times S(\mathfrak{h})$ into $S(\mathfrak{m})$. Moreover $\zeta(H)$ is real and equal to $\pm\prod_{\alpha\in Q'}(\alpha(H))^2$ if $H\in\mathfrak{h}_0$. Therefore by applying Lemmas 7 and 8 to $\mathfrak{m}_0$ (instead of $\mathfrak{g}_0$), we conclude that

$$(|\zeta|^{-\frac{1}{2}}\partial(p_\mathfrak{m})\circ|\zeta|^{\frac{1}{2}})_{H_0}-(\pi^{-1}\partial(\bar{p})\circ\pi)_{H_0}\in\partial(\Gamma_{H_0}(\mathfrak{S}_\mathfrak{m}'\times S(\mathfrak{h}))),$$

where $\bar{p}$ is the restriction of p (and therefore also of $p_\mathfrak{m}$) on $\mathfrak{h}$. On the other hand, it follows from the definition of $\Delta(p)$ that

$$(\Delta(p))_{H_0}-\partial(p)\in\partial(\Gamma_{H_0}(\mathfrak{Q}'\times S(\mathfrak{m}))).$$

Therefore

$$D_{H_0}\equiv\partial(p)-(\pi^{-1}\partial(\bar{p})\circ\pi)_{H_0}\equiv 0 \mod \partial(\Gamma_{H_0}(\mathfrak{S}'\times S(\mathfrak{m})))$$

from Lemma 8. Now it is an immediate consequence of the defintion of Γ_Y $(Y \in \mathfrak{g}_0)$ that $\Gamma_Y(b_1 b_2 \times \mathrm{q}) = \Gamma_Y(b_1 \times \Gamma_Y(b_2 \times q))$ $(b_1, b_2 \in \mathfrak{B}, q \in S(\mathfrak{g}))$. Therefore, since $S(\mathfrak{m}) = \Gamma_{H_0}(\mathfrak{S}_{\mathfrak{m}} \times S(\mathfrak{h}))$, it follows that $\Gamma_{H_0}(\mathfrak{S}' \times S(\mathfrak{m})) \subset \Gamma_{H_0}(\mathfrak{B}' \times S(\mathfrak{h}))$, where $\mathfrak{B}' = \mathfrak{B}\mathfrak{g}$. But $\mathfrak{B}' = \mathfrak{S}' + \mathfrak{B}\mathfrak{h}$ and $\Gamma_{H_0}(\mathfrak{B}\mathfrak{h} \times S(\mathfrak{h})) = \{0\}$. Therefore $\Gamma_{H_0}(\mathfrak{B}' \times S(\mathfrak{h})) = \Gamma_{H_0}(\mathfrak{S}' \times S(\mathfrak{h}))$. This proves that $\Gamma_{H_0}(\mathfrak{S}' \times S(\mathfrak{m})) = \Gamma_{H_0}(\mathfrak{S}' \times S(\mathfrak{h}))$, and hence $D_{H_0} \in \partial(S(\mathfrak{m}) \cap \Gamma_{H_0}(\mathfrak{S}' \times S(\mathfrak{h})))$. But, as we have seen, $S(\mathfrak{m}) = \Gamma_{H_0}(\mathfrak{S}_{\mathfrak{m}} \times \mathrm{SA}\mathfrak{h}))$ and Γ_{H_0} is univalent on $\mathfrak{S} \times S(\mathfrak{h})$ (Lemma 4). Therefore

$$D_{H_0} \in \partial(\Gamma_{H_0}(\mathfrak{S}_{\mathfrak{m}}' \times S(\mathfrak{h})) \subset \partial(\Gamma_{H_0}(\mathfrak{M}' \times S(\mathfrak{m}))),$$

and so the lemma is proved.

COROLLARY. *If* $H \in \mathfrak{h}_0'$ *then*

$$(\Delta(p))_H - (\pi^{-1}\partial(\bar{p}) \circ \pi)_H \in \partial(\Gamma_H(\mathfrak{M}' \times S(\mathfrak{h})))$$

for $p \in I(\mathfrak{g})$.

For, in view of what we have seen above, the left side lies in

$$\partial(S(\mathfrak{m}) \cap \Gamma_H(\mathfrak{S}' \times S(\mathfrak{m}))) \text{ and } S(\mathfrak{m}) \cap \Gamma_H(\mathfrak{S}' \times S(\mathfrak{m})) \subset \Gamma_H(\mathfrak{M}' \times S(\mathfrak{h})).$$

8. Closer study of a special case. Define $\mathfrak{k}_0$ and $\mathfrak{p}_0$ as in [4(c), §2] adn let $\mathfrak{k}, \mathfrak{p}$ denote their respective complexifications in $\mathfrak{g}$. *Throughout this section we shall assume that* $\mathfrak{h}_0 \subset \mathfrak{k}_0$. Then the theory developed in Section 7 can be applied to $\mathfrak{m}_0 = \mathfrak{k}_0$. In this case $\mathfrak{q}_0 = \mathfrak{p}_0$ and $\zeta(X) = \det(\operatorname{ad} X)_{\mathfrak{p}}$ $(X \in \mathfrak{k})$, where $(\operatorname{ad} X)_{\mathfrak{p}}$ is the restriction of $\operatorname{ad} X$ on $\mathfrak{p}$. Put $\mathfrak{P} = \lambda(S(\mathfrak{p}))$. Then we intend to prove the following result concerning the Casimir polynomial ω of $\mathfrak{g}$.

LEMMA[14] 24. *There exists a unique polynomial mapping* γ_ω *of* $\mathfrak{k}$ *into* $\mathfrak{P} \times S(\mathfrak{k})$ *such that* $\Gamma_X(\gamma_\omega(X)) = \zeta(X)\omega$ $(X \in \mathfrak{k}_0)$. *Moreover* $(\gamma_\omega(X))^k = \gamma_\omega(kX)$ *for* $k \in K$ *and* $X \in \mathfrak{k}$.

The case $\mathfrak{g}_0 = \mathfrak{k}_0$ being trivial, we assume that $\mathfrak{p}_0 \neq 0$. Let P_- and P_0 be the sets of all compact and all noncompact roots in P, respectively (see [4(g), p. 751]). Then if r is the number of roots in P_0, $\dim \mathfrak{p} = 2r$. Let t be an indeterminate and consider the polynomial

$$\prod_{\beta \in P_0} (t - \beta^2) = t^r + q_1 t^{r-1} + \cdots + q_r$$

with coefficients $q_i \in S(\mathfrak{h})$. Let $W_{\mathfrak{k}}$ be the subgroup of the Weyl group W

---

[14] The results of this section are quite similar to those of [4(e), §10].

generated by the reflexions s_α corresponding to $\alpha \in P_-$. Then, since $\mathfrak{k}$ is reductive (Lemma 5 of [4(c)]), $W_\mathfrak{k}$ can also be regarded as the Weyl group of $\mathfrak{k}$ with respect to $\mathfrak{h}$ (see [4(e), §6]). Let K denote the analytic subgroup of G corresponding to $\mathfrak{k}_0$ and $I(\mathfrak{k})$ the set of those $p \in S(\mathfrak{k})$ which are invariant under K. Similarly, let $I_\mathfrak{k}(\mathfrak{h})$ be the set of all elements in $S(\mathfrak{h})$ which are invariant under $W_\mathfrak{k}$. Then Chevalley's Theorem (Lemma 9) is obviously applicable to $(\mathfrak{k}, \mathfrak{h})$ in place of $(\mathfrak{g}, \mathfrak{h})$. Hence $p \to \bar{p}$ $(p \in I(\mathfrak{k}))$ is an isomorphism of $I(\mathfrak{k})$ onto $I_\mathfrak{k}(\mathfrak{h})$. Now if β is a noncompact root and $s \in W_\mathfrak{k}$, then $s\beta$ is also noncompact (see the proof of Lemma 10 of [4(g)]). From this it follows that $q_i \in I_\mathfrak{k}(\mathfrak{h})$, $1 \leqq i \leqq r$. Hence we can select $\sigma_i \in I(\mathfrak{k})$ such that $q_i = \bar{\sigma}_i$. For any $X \in \mathfrak{k}$, put $S(X) = (\mathrm{ad}\, X)_\mathfrak{p}^2$. Then we shall first prove the following lemma.

LEMMA 25. $\sigma_r = \zeta$ *and*

$$(S(X))^r + \sigma_1(X)(S(X))^{r-1} + \cdots + \sigma_r(X) I_\mathfrak{p} = 0 \qquad (X \in \mathfrak{k}).$$

(Here $I_\mathfrak{p}$ is the identity mapping of $\mathfrak{p}$.)

It is clear that $\zeta \in I(\mathfrak{k})$ and $\bar{\zeta} = (-1)^r \prod_{\beta \in P_0} \beta^2 = q_r$. Therefore, in view of the above *isomorphism* of $I(\mathfrak{k})$ onto $I_\mathfrak{k}(\mathfrak{h})$, we can conclude that $\zeta = \sigma_r$. Moreover $\tau : X \to \{(S(X))^r + \sigma_1(X)(S(X))^{r-1} + \cdots + \sigma_r(X) I_\mathfrak{p}\}$ $(X \in \mathfrak{k})$ is obviously a polynomial mapping of $\mathfrak{k}$ into the space of endomorphisms of $\mathfrak{p}$, and therefore it would be sufficient to prove that τ maps $\mathfrak{k}_0$ into zero. Moreover, since K is compact [7], $\mathfrak{k}_0 = \bigcup_{k \in K} k\mathfrak{h}_0$, and so it would clearly be enough to show that τ maps $\mathfrak{h}_0$ into zero. But if $H \in \mathfrak{h}$, $S(H)$ is semisimple and all its eigenvalues are of the form $\beta(H)^2$ $(\beta \in P_0)$. Therefore

$$\tau(H) = \prod_{\beta \in P_0} (S(H) - \beta(H)^2 I_\mathfrak{p}) = 0,$$

and this proves our assertion.

Now put

$$T(X) = -\{(S(X))^{r-1} + \sigma_1(X)(S(X))^{r-2} + \cdots + \sigma_{r-1}(X) I_\mathfrak{p}\} \qquad (X \in \mathfrak{k}),$$

so that $S(X)T(X) = T(X)S(X) = \zeta(X) I_\mathfrak{p}$. Select a base $Y_1, \cdots, Y_p$ $(p = 2r)$ for $\mathfrak{p}$ over C. Since $\mathfrak{k}$ and $\mathfrak{p}$ are orthogonal under B, B is nondegenerate on $\mathfrak{p}$. Hence we can choose $Y_i' \in \mathfrak{p}$ $(1 \leqq i \leqq p)$ such that $B(Y_i', Y_j) = \delta_{ij}$ $(1 \leqq i, j \leqq p)$. Let $\omega_\mathfrak{k}$ and $\omega_\mathfrak{p}$ denote the restrictions of ω on $\mathfrak{k}$ and $\mathfrak{p}$, respectively. Then in view of the above-mentioned orthogonality of $\mathfrak{k}$ and $\mathfrak{p}$, $\omega = \omega_\mathfrak{k} + \omega_\mathfrak{p}$. Moreover, it is easy to see that $\omega_\mathfrak{p} = \sum_{1 \leqq i \leqq p} Y_i Y_i'$.

Now fix an element $X \in \mathfrak{k}$ and let S', T' be two linear transformations of $\mathfrak{p}$ which commute with $(\mathrm{ad}\,X)_{\mathfrak{p}}$. Put $U_i = S'Y_i$, $V_i = T'Y_i$, $U_i' = S'Y_i'$, $V_i' = T'Y_i'$ $(1 \leqq i \leqq p)$. Note that $Z = \sum_{1 \leqq i \leqq p} B(Z, Y_i')Y_i = \sum_{1 \leqq i \leqq p} B(Z, Y_i)Y_i'$ $(Z \in \mathfrak{p})$, and therefore $(\mathrm{ad}\,X)Z = -\sum_i B(Z, (\mathrm{ad}\,X)Y_i')Y_i$. Hence

$$(\mathrm{ad}\,X)U_i = S'(\mathrm{ad}\,X)Y_i = -\sum_j B(Y_i, (\mathrm{ad}\,X)Y_j')U_j,$$

$$(\mathrm{ad}\,X)V_i' = T'(\mathrm{ad}\,X)Y_i' = \sum_j B((\mathrm{ad}\,X)Y_i', Y_j)V_j',$$

and so if we consider the tensor product $\mathfrak{p} \times \mathfrak{p}$, it follows that

$$\sum_i ((\mathrm{ad}\,X)U_i) \times V_i' = -\sum_{i,j} B(Y_i, (\mathrm{ad}\,X)Y_j')U_j \times V_i' = -\sum_j U_j \times (\mathrm{ad}\,X)V_j'.$$

Obviously, this implies that

$$\sum_i [X, U_i]V_i' = -\sum_i U_i[X, V_i'],$$

$$\sum_i [[X, U_i], V_i'] = -\sum_i [U_i, [X, V_i']].$$

Now put $Y_j(X) = T(X)Y_j$ $(1 \leqq j \leqq p)$ so that $S(X)Y_j(X) = \zeta(X)Y_j$. Then if $U, V \in \mathfrak{p}$ and $X \in \mathfrak{k}_0$,

$$\Gamma_X(U \cdot V \times 1) = (L_{[U,X]} + d_U)[V, X] = [X, U][X, V] - [U, [X, V]]$$

in the notation of Section 3. Hence

$$\sum_{1 \leqq j \leqq p} \Gamma_X(Y_j' \cdot Y_j(X) \times 1) = \sum_j [X, Y_j'][X, Y_j(X)] - \sum_j [Y_j', [X, Y_j(X)]].$$

But since $(\mathrm{ad}\,X)_{\mathfrak{p}}T(X)$ commutes with $(\mathrm{ad}\,X)_{\mathfrak{p}}$, it follows from our result above that

$$\sum_j [X, Y_j'][X, Y_j(X)] = -\sum_j Y_j'(S(X)Y_j(X)) = -\zeta(X)\omega_{\mathfrak{p}},$$

and therefore

$$\sum_{1 \leqq j \leqq p} \Gamma_X(Y_j' \cdot Y_j(X) \times 1) = -\zeta(X)\omega_{\mathfrak{p}} - \sum_j [Y_j', [X, Y_j(X)]].$$

Now put $b(X) = -\frac{1}{2}\sum_i (Y_i' \cdot Y_i(X) + Y_i(X) \cdot Y_i')$ $(X \in \mathfrak{k})$. Then $b(X) \in \mathfrak{P}$ and $b(X) = -\sum_j Y_j' \cdot Y_j(X) + \frac{1}{2}\sum_j [Y_j', Y_j(X)]$. Moreover, it follows from our result above that

$$\sum_j [(\mathrm{ad}\,X)Y_j', Y_j(X)] = -\sum_j [Y_j', (\mathrm{ad}\,X)Y_j(X)],$$

and therefore $\Gamma_X(b(X)\times 1)=\zeta(X)\omega_{\mathfrak{p}}+\sum_j [Y_j', [X, Y_j(X)]]$ $(X\in\mathfrak{k}_0)$. Put $Z(X)=\sum_j [Y_j', [X, Y_j(X)]]$ and

$$\gamma_\omega(X)=b(X)\times 1+\zeta(X)(1\times\omega_{\mathfrak{k}})-(1\times Z(X)) \qquad (X\in\mathfrak{k}).$$

Then $Z(X)\in[\mathfrak{p},\mathfrak{p}]\subset\mathfrak{k}$, and therefore $\gamma_\omega(X)\in\mathfrak{P}\times S(\mathfrak{k})$. Moreover,

$$\Gamma_X(\gamma_\omega(X))=\zeta(X)\omega_{\mathfrak{p}}+\zeta(X)\omega_{\mathfrak{k}}=\zeta(X)\omega \qquad (X\in\mathfrak{k}_0)$$

and it is clear from its definition that γ_ω is a polynomial mapping of $\mathfrak{k}$ into $\mathfrak{P}\times S(\mathfrak{k})$. We still have to prove its uniqueness.

Let $\mathfrak{k}_0'$ be the set of all points $X\in\mathfrak{k}_0$ where $\zeta(X)\neq 0$. It follows from Lemma 20 that γ_ω is completely determined on $\mathfrak{k}_0'$ by the condition $\Gamma_X(\gamma_\omega(X))=\zeta(X)\omega$. But it is obvious that two polynomial mappings of $\mathfrak{k}$ must be identical if they coincide on some nonempty open subset of $\mathfrak{k}_0$. This proves that γ_ω is unique.

For a fixed $k\in K$, consider the mapping $\gamma_\omega': X\rightarrow(\gamma_\omega(kX))^{k^{-1}}$ $(X\in\mathfrak{k})$. It is clear that γ_ω' is a polynomial mapping which, in view of Lemma 22, must coincide with γ_ω on $\mathfrak{k}_0'$. Hence $\gamma_\omega'=\gamma_\omega$, and therefore $(\gamma_\omega(X))^k$ $(k\in K, X\in\mathfrak{k})$. This completes the proof of Lemma 24.

We can now define a differential operator D on $\mathfrak{k}_0$ by

$$D_X=\zeta(X)\partial(\omega_{\mathfrak{k}})-\partial(Z(X)) \qquad (X\in\mathfrak{k}_0)$$

in the above notation. It is clear that $D\in\mathfrak{D}(\mathfrak{k})$ and it follows from Lemma 24 that D is invariant under K. Finally, it is obvious from the defintion of $\Delta(\omega)$ (in Lemma 23) that $D=\zeta\Delta(\omega)$ on $\mathfrak{k}_0'$. Let D^* denote the adjoint of D.

LEMMA 26. *Let $I^\infty(\mathfrak{k}_0)$ denote the set of all functions $f\in C^\infty(\mathfrak{k}_0)$ which are invariant under K. Then $Df=D^*f$ for $f\in I^\infty(\mathfrak{k}_0)$.*

Let f be a fixed element in $I^\infty(\mathfrak{k}_0)$. We have to prove that $Df-D^*f=0$. Since D is invariant under K, the same holds for D^*, and therefore $Df-D^*f$ lies in $I^\infty(\mathfrak{k}_0)$. Hence, in view of the fact that $\mathfrak{k}_0=\bigcup_{k\in K}(k\mathfrak{h}_0)$, it would be enough to prove that $Df-D^*f$ is zero on $\mathfrak{h}_0'$. Let H_0 be any point in $\mathfrak{h}_0'$ and select an open connected neighborhood U of H_0 in $\mathfrak{h}_0'$. Then $V=\bigcup_{k\in K}(kU)$ is an open connected neighborhood of H_0 in $\mathfrak{k}_0$. Let dX denote the Euclidean measure on $\mathfrak{k}_0$. It is obvious that if $g\in C_c^\infty(V)$,

$$\int_V (Df-D^*f)g\,dX=\int_V (Df-D^*f)g_1\,dX,$$

where $g_1(X) = \int_K g(kX)\,dk$ $(X \in V)$ and dk is the normalized Haar measure on K. Therefore, in order to prove that $Df - D^*f$ is zero on V, it is sufficient to show that

$$\int (Df)\phi\, dX = \int f(D\phi)\,dX$$

for every $\phi \in I^\infty(\mathfrak{k}_0)$ which vanishes outside some compact set in V. Fix such a function ϕ. Now $V \subset \mathfrak{k}_0'$ and therefore $D = \zeta\Delta(\omega)$ on V. Moreover since ζ takes only nonzero real values on the connected set V, it must keep constant sign. Hence it follows from Lemma 23 that

$$\psi(X;D) = \epsilon\psi(X; |\zeta|^{\frac{1}{2}}\partial(\omega_{\mathfrak{k}}) \circ |\zeta|^{\frac{1}{2}}) \qquad (X \in V, \psi \in I^\infty(\mathfrak{k}_0)),$$

where $\epsilon = 1$ or -1 according as ζ is positive or negative on V. Therefore, if $f' = |\zeta|^{\frac{1}{2}} f$ and $\phi' = |\zeta|^{\frac{1}{2}}\phi$, we have only to show that

$$\int (\partial(\omega_{\mathfrak{k}})f')\phi'\,dX = \int f'(\partial(\omega_{\mathfrak{k}})\phi')\,dX.$$

But, $\omega_{\mathfrak{k}}$ being a homogeneous polynomial of degree 2, $\partial(\omega_{\mathfrak{k}})$ is self-adjoint. Moreover, $\phi' \in C_c^\infty(V)$ and f' is of class C^∞ on V. Therefore the above relation is obvious, and so the lemma is proved.

Since every root α takes only pure imaginary values on $\mathfrak{h}_0$, it is clear that the corresponding Weyl reflexion s_α maps $\mathfrak{h}_0$ into itself. Hence $s\mathfrak{h}_0 = \mathfrak{h}_0$ for any $s \in W$. Put $J(\mathfrak{k}_0) = I^\infty(\mathfrak{k}_0) \cap \mathcal{B}(\mathfrak{k}_0)$ and consider the $\mathcal{B}$-topology on $J(\mathfrak{k}_0)$.

LEMMA 27. *For any $f \in \mathcal{B}(\mathfrak{h}_0)$, there exists exactly one element $\psi_f \in I^\infty(\mathfrak{k}_0)$ such that $\pi(H)\psi_f(H) = \sum_{s \in W} \epsilon(s)f(sH)$ $(H \in \mathfrak{h}_0)$. Furthermore, ψ_f lies in $J(\mathfrak{k}_0)$ and $f \to \psi_f$ is a continuous mapping of $\mathcal{B}(\mathfrak{h}_0)$ into $J(\mathfrak{k}_0)$.*

Since $\mathfrak{k}_0 = \bigcup_{k \in K} k\mathfrak{h}_0$, a function in $I^\infty(\mathfrak{k}_0)$ is completely determined by its restriction on $\mathfrak{h}_0'$. Therefore the uniqueness of ψ_f is obvious. Now put $\mathfrak{u} = \mathfrak{k}_0 + (-1)^{\frac{1}{2}}\mathfrak{p}_0$. Then $\mathfrak{u}$ is a compact real form of $\mathfrak{g}$. Let U be the (connected) adjoint group of $\mathfrak{u}$ and let $J(\mathfrak{u})$ denote the set of all functions in $\mathcal{B}(\mathfrak{u})$ which are invariant under U. We consider the $\mathcal{B}$-topology on $J(\mathfrak{u})$. Then from Lemma 17, there exists, for each $f \in \mathcal{B}(\mathfrak{h}_0)$, a unique element $\Psi_f \in J(\mathfrak{u})$ such that

$$\pi(H)\Psi_f(H) = \sum_{s \in W} \epsilon(s)f(sH) \qquad (H \in \mathfrak{h}_0)$$

and $f \to \Psi_f$ is a continuous mapping of $\mathcal{B}(\mathfrak{h}_0)$ into $J(\mathfrak{u})$. Let σ denote the mapping of $\mathcal{B}(\mathfrak{u})$ into $\mathcal{B}(\mathfrak{k}_0)$ which assigns to any function its restriction on $\mathfrak{k}_0$. It is obvious that σ is continuous and it maps $J(\mathfrak{u})$ into $J(\mathfrak{k}_0)$. Therefore $f \to \psi_f = \sigma\Psi_f$ is a continuous mapping of $\mathcal{B}(\mathfrak{h}_0)$ into $J(\mathfrak{k}_0)$ and ψ_f satisfies the condition of the lemma.

Put $I_c^\infty(\mathfrak{k}_0) = I^\infty(\mathfrak{k}_0) \cap C_c^\infty(\mathfrak{k}_0)$, and consider $C_c^\infty(\mathfrak{h}_0)$ and $I_c^\infty(\mathfrak{k}_0)$ under the C_c^∞-topology. If Ω is any compact set in $\mathfrak{h}_0$ and f a function in $C_c^\infty(\mathfrak{h}_0)$ whose carrier lies in Ω, then it is obvious that the carrier of ψ_f is contained in $\Omega' = \bigcup_{k \in K} k\Omega$. Since Ω' is compact, it follows that $\psi_f \in I_c^\infty(\mathfrak{k}_0)$ and $f \to \psi_f$ $(f \in C_c^\infty(\mathfrak{h}_0))$ is a continuous mapping of $C_c^\infty(\mathfrak{h}_0)$ into $I_c^\infty(\mathfrak{k}_0)$.

LEMMA 28. *$D\psi_f = \zeta\psi_{\partial(\bar{\omega})f}$ for all $f \in \mathcal{B}(\mathfrak{h}_0)$.*

It is sufficient to prove that $D\psi_f - \zeta\psi_{\partial(\bar{\omega})f}$ is zero on $\mathfrak{h}_0'$. Select a point $H_0 \in \mathfrak{h}_0'$. We know that $D = \zeta\Delta(\omega)$ on $\mathfrak{k}_0'$, and therefore it follows from the Corollary of Lemma 23 that

$$\psi_f(H_0; D) = \zeta(H_0)\psi_f(H_0; \Delta(\omega)) = \zeta(H_0)\pi(H_0)^{-1}g(H_0; \partial(\bar{\omega})),$$

where g is the function on $\mathfrak{h}_0$ given by

$$g(H) = \pi(H)\psi_f(H) = \sum_{s \in W} \epsilon(s) f^s(H) \qquad (H \in \mathfrak{h}_0).$$

On the other hand, $(\partial(\bar{\omega})f)^s = \partial(\bar{\omega})f^s$ $(s \in W)$ since $\bar{\omega} \in I(\mathfrak{h})$, and therefore $\partial(\bar{\omega})g = \sum_{s \in W} \epsilon(s)(\partial(\bar{\omega})f)^s$. This proves that

$$g(H; \partial(\bar{\omega})) = \pi(H)\psi_{\partial(\bar{\omega})f}(H) \qquad (H \in \mathfrak{h}_0),$$

and therefore $\psi_f(H_0; D) = \zeta(H_0)\psi_{\partial(\bar{\omega})f}(H_0)$.

Let τ be a distribution on $\mathfrak{k}_0$ which is invariant under K. Then we define a distribution Φ on $\mathfrak{h}_0$ by $\Phi(f) = \tau(\zeta\psi_f)$ $(f \in C_c^\infty(\mathfrak{h}_0))$. Notice that if τ is a $\mathcal{B}$-distribution, the same holds for Φ. The following theorem is the main result of this section.

THEOREM 5.[15] *Suppose there exists a complex number c such that $D\tau = c\zeta\tau$. Then Φ coincides with an analytic function on $\mathfrak{h}_0$.*

Let f be a function in $C_c^\infty(\mathfrak{h}_0)$. Then $\tau(D^*\psi_f) = \tau(D\psi_f) = \Phi(\partial(\bar{\omega})f)$ from Lemmas 26 and 28. But $\tau(D^*\psi_f) = c\tau(\zeta\psi_f) = c\Phi(f)$ since $D\tau = c\zeta\tau$. Therefore Φ satisfies the differential equation $\partial(\bar{\omega})\Phi - c\Phi = 0$. But since $\mathfrak{h}_0 \subset \mathfrak{k}_0$, $\bar{\omega}$ is a negative-definite quadratic form on $\mathfrak{h}_0$ and so this equation is of the elliptic type. Hence we can conclude (see [8(I), p. 136] and [5]) that Φ is an analytic function on $\mathfrak{h}_0$.

---

[15] Compare this with Theorem 5 of [4(e)].

We shall see in another paper that the above theorem plays an essential role in the theory of Fourier transforms on a noncompact semisimple Lie algebra.

INSTITUTE FOR ADVANCED STUDY,
COLUMBIA UNIVERSITY.

REFERENCES.

[1] P. Cartier, Séminaire "Sophus Lie," 1954-55, Ecole Normale Supérieure, Paris.

[2] C. Chevalley, *Amer. Jour. Math.*, vol. 77 (1955), pp. 778-782.

[3] L. Gårding, *Math. Scand.*, vol. 1 (1953), pp. 55-72.

[4] Harish-Chandra, (a) *Ann. of Math.*, vol. 50 (1949), pp. 900-915.
(b) *Trans. Amer. Math. Soc.*, vol. 70 (1951), pp. 28-96.
(c) " " " " vol. 75 (1953), pp. 185-243.
(d) " " " " vol. 76 (1954), pp. 485-528.
(e) " " " " vol. 83 (1956), pp. 98-163.
(f) *Bull. Amer. Math. Soc.*, vol. 61 (1955), pp. 389-396.
(g) *Amer. Jour. Math.*, vol. 77 (1955), pp. 743-777.
(h) *Proc. Nat. Acad. Sci., U.S.A.*, vol. 42 (1956), pp. 252-253.
(i) " " " " " vol. 42 (1956), pp. 538-540.

[5] F. John, *Proceedings of the symposium on spectral theory and differential problems*, Stillwater, Okla. (1951), pp. 113-175.

[6] J. L. Koszul, *Bull. Soc. Math. France*, vol. 78 (1950), pp. 65-127.

[7] G. D. Mostow, *Bull. Amer. Math. Soc.*, vol. 55 (1949), pp. 969-980.

[8] L. Schwartz, *Théorie des distributions*, I (1950), II (1951), Paris, Hermann.

[9] H. Weyl, *The structure and representations of continuous groups*, Princeton, The Institute for Advanced Study, 1935.

SUR LA CLASSIFICATION DES FIBRES HOLOMORPHES SUR LA SPHERE DE RIEMANN.*

par A. GROTHENDIECK.[1]

Par. 1. Enoncé du théorême principal. Soit X une variété holomorphe (ou plus généralement un "espace analytique" [6]), nous considérons des fibrés holomorphes sur X, de groupe structural un groupe de Lie complexe G. Soit $\boldsymbol{O}_X(G)$ le faisceau des germes d'applications holomorphes de X dans G, (c'est un faisceau de groupes, en général non commutatifs), nous désignerons par $H^1(X, \boldsymbol{O}_X(G))$ l'ensemble des classes de fibrés holomorphes sur X, de groupe structural G. (Pour tout ce qui concerne la notation $H^1(X, \boldsymbol{F})$—où $\boldsymbol{F}$ est un faisceau de groupes non nécessairement commutatifs sur X—et son mécanisme algébrique, voir [4]). Nous n'exigeons pas que G soit connexe, et désignerons par G_0 la composante connexe de l'élément neutre, par $\mathfrak{G}$ son algèbre de Lie. G est dit *réductif* si son algèbre de Lie $\mathfrak{G}$ est réductive, c'est à dire somme directe de son centre et d'une algèbre semi-simple. Par abus de langage, nous appellerons *sous-groupe de Cartan* H de G un sous-groupe holomorphe *connexe* ayant pour algèbre de Lie une sous-algèbre de Cartan $\mathfrak{h}$ de $\mathfrak{G}$. Si G est un groupe algèbrique connexe, cette terminologie coïncide avec elle de [3]. Si Z est le centre de G_0, alors H contient Z_0, et H est l'image réciproque d'un sous-groupe de Cartan H_1 du groupe $G_1 = G_0/Z_0$ (qui est semi-simple dans le cas où G est réductif), D'après la définition générale des sous-algèbres de Cartan [3], si N est le normalisateur de H dans G, le quotient $W = N/H$ est un groupe discret (et même fini si G/G_0 est fini), on l'appelle le *groupe de Weyl* de G.

Tout fibré holomorphe de groupe structural H définissant un fibré holomorphe associé de groupe structural G, on obtient une application canonique $H^1(X, \boldsymbol{O}_X(H)) \rightarrow H^1(X, \boldsymbol{O}_X(G))$. D'autre part, N opère par automorphismes intérieurs dans G et H est stable sous ces opérations, d'où d'ensuit que N opère aussi dans les ensembles $H^1(X, \boldsymbol{O}_X(H))$ et $H^1(X, \boldsymbol{O}_X(G))$ et l'application précédente est compatible avec ces opérations. D'ailleurs les opérations sur le deuxième ensemble, correspondant à des automorphismes

---

* Received October 12, 1956.

[1] **La majeure partie de ce travail a été faite en 1955 alors que l'auteur était Visiting Associate Professor à l'Université de Kansas, USA.**

intérieurs de G, sont triviales, et pour la même raison les éléments de H opèrent trivialement sur $H^1(X, \boldsymbol{O}_X(H))$, de sorte qu'en fait le groupe de Weyl $W = N/H$ opère sur cet ensemble. On en déduit une application canonique

$$H^1(X, \boldsymbol{O}_X(H))/W \to H^1(X, \boldsymbol{O}_X(G)) \tag{1}$$

où le premier membre désigne l'ensemble des trajectoires dans $H^1(X, \boldsymbol{O}_X(H))$ sous le groupe de Weyl. L'image de cette application est l'ensemble des classes de fibrés holomorphes de groupe G dont le groupe structural peut se réduire au sous-groupe de Cartan H. Le but du présent travail est la démonstration du

THÉORÈME 1.1. *Soit G un groupe de Lie complexe réductif, soit X la sphère de Riemann (c'est à dire une courbe algèbrique complète de genre 0). Alors l'application* (1) *est bijective, en d'autres termes: Pour tout fibré holomorphe sur X de groupe structural G, le groupe structural peut se réduire au sous-groupe de Cartan H de G, et ceci de façon unique à une opération du groupe de Weyl W près.*

On peut expliciter ce résultat ainsi. On sait, puisque G est réductif, que H est abélien, soit $\mathfrak{h}$ son algèbre de Lie. L'homomorphisme $h \to \exp. 2i\pi h$ de $\mathfrak{h}$ sur H identifie l'espace vectoriel $\mathfrak{h}$ à un groupe de recouvrement de H, soit P son noyau ("réseau unité" de $\mathfrak{h}$). La suite exacte $0 \to P \to \mathfrak{h} \to H \to 0$ donne une suite exacte de faisceaux abéliens $0 \to P \to \boldsymbol{O}_X(\mathfrak{h}) \to \boldsymbol{O}_X(H) \to 0$ d'où une suite exacte de cohomologie

$$H^1(X, \boldsymbol{O}_X(\mathfrak{h})) \to H^1(X, \boldsymbol{O}_X(H)) \to H^2(X, P) \to H^2(X, \boldsymbol{O}_X(\mathfrak{h})).$$

Or il est bien connu que $H^i(X, \boldsymbol{O}_X) = 0$ pour $i \geqq 1$ ($\boldsymbol{O}_X$ étant le faisceau des germes de fonctions holomorphes sur X) : c'est vrai chaque fois que X est un espace projectif complexe [5]. Par suite on a aussi $H^i(X, \boldsymbol{O}_X(\mathfrak{h})) = 0$, d'où

$$H^1(X, \boldsymbol{O}_X(H)) \approx H^2(X, P) \approx P. \tag{2}$$

Ces isomorphismes sont "fonctoriels," et en particulier compatibles avec les opérations de W, donc on obtient:

COROLLAIRE 1. *Sous les conditions du théorème* 1.1, *l'ensemble $H^1(X, \boldsymbol{O}_X(G))$ s'identifie à l'ensemble P/W, où P est le réseau unité dans l'algèbre de Cartan $\mathfrak{h}$ correspondant au groupe de Cartan H, et W le groupe de Weyl correspondant à H.*

Supposons pour simplifier que G est connexe et semi-simple, considérons un système fondamental de racines $(\alpha_i)_{1 \leqq i \leqq r}$ sur $\mathfrak{h}$ [2], et la "chambre de Weyl" C formée des $h \in \mathfrak{h}$ tels que $\alpha_i(h) \geqq 0$ pour tout i. On sait que tout élément h de $\mathfrak{h}$ tel que $\alpha_i(h)$ soit réel pour tout i, est conjugué sous W à un élément et un seul de C (savoir le plus grand des transformés de h par W, dans l'ordre lexicographique relatif à une certaine base de $\mathfrak{h}$ [2]). Donc:

COROLLAIRE 2. *Si G est connexe semi-simple, alors $H^1(X, \boldsymbol{O}_X(G))$ s'identifie à l'ensemble des éléments du réseau unité P de G relativement à $\mathfrak{h}$ qui sont dans le chambre de Weyl C.*

En un certain sens, la classification des fibrés holomorphes sur la sphère de Riemann X, de groupe G, est duale de la classification des représentations linéaires de dimension finie de G [2]. On peut préciser ce point en donnant un énoncé équivalent du théorème 1.1 ne faisant plus intervenir de sous-group de Cartan. Pour ceci, rappelons d'abord que le groupe $H^1(X, \boldsymbol{O}_X(\boldsymbol{C}^*))$ des classes de fibrés de groupe $\boldsymbol{C}^*$[2] sur une variété projective X, s'identifie au groupe des classes de diviseurs sur X mod les diviseurs principaux, donc au group Z des entiers rationnels quand X est la sphère de Riemann. Soit dans ce cas L_1 le fibré vectoriel holomorphe sur X, de fibré $\boldsymbol{C}$ et de groupe $\boldsymbol{C}^*$, correspondant à un diviseur de degré 1. Si G est un groupe de Lie complexe quelconque, et u un homomorphisme complexe de $\boldsymbol{C}$ dans G, on peut considérer le fibré holomorphe de groupe structural G associé à L_1 et à u. La classe de ce fibré ne change évidemment pas si on remplace u par ${}^g u(t) = gu(t)g^{-1}$ (car, comme on l'a déjà remarqué, la permutation de $H^1(X, \boldsymbol{O}_X(G))$ définie par un automorphisme intérieur de G est l'identité). En d'autres termes, désignant par $\mathrm{Hom}(\boldsymbol{C}^*, G)/G$ l'ensemble des classes de homomorphismes complexes de $\boldsymbol{C}^*$ dans G, mod composition avec des automorphismes intérieurs de G, on obtient une application naturelle

$$\mathrm{Hom}(\boldsymbol{C}^*, G)/G \to H^1(X, \boldsymbol{O}_X(G)). \tag{3}$$

THÉORÈME 1.2. *Soit X la sphère de Riemann, G un groupe de Lie complexe réductif. Alors l'application (3) est bijective. En d'autres termes, tout fibré holomorphe sur X de groupe G est associé au fibré fondamental L_1 et à un homomorphisme complexe u de $\boldsymbol{C}^*$ dans G, et ce dernier est unique mod. composition avec un automorphisme intérieur de G.*

La démonstration des théorèmes 1.1 et 1.2 sera développée dans les par. 2, 3, 4. Nous allons ici d'abord montrer que le théorème 1.2 est bien équivalent au théorème 1.1. Prouvons d'abord que le th. 1.2 est vrai si G est un groupe *abélien connexe* H. Considérons alors le diagramme

---

[2] C désigne le corps des complexes, C^* le groupe complexe multiplicatif des nombres complexes $\neq 0$.

$$\begin{tikzcd}
\operatorname{Hom}(\mathbf{C}^*,H) \arrow[rr] & & H^1(X,\boldsymbol{O}_X(H)) \arrow[dl] \\
& P \arrow[ul] &
\end{tikzcd}$$

où P est le réseau unité de l'algèbre de Lie $\mathfrak{h}$ de H, où l'homomorphisme horizontal est celui envisagé dans le th. 1.2, et l'homomorphisme vertical droit est l'isomorphisme (2). Le troisième homomorphisme $P \rightarrow \operatorname{Hom}(\mathbf{C}^*,H)$ est aussi un isomorphisme, obtenu en remarquant que les homomorphismes complexes de $\mathbf{C}^* \approx \mathbf{C}/\mathbf{Z}$ dans $H \approx \mathfrak{h}/P$ correspondent biunivoquement aux homomorphismes de $\mathbf{C}$ dans $\mathfrak{h}$ appliquant Z dans P, c'est-à-dire aux éléments de P. Le diagramme ainsi obtenu est commutatif, comme on voit aussitôt, d'où résulte que l'homomorphisme horizontal est lui aussi bijectif.—Passons au cas général où on a un groupe de Lie complexe réductif G quelconque. On a un diagramme commutatif d'applications naturelles:

$$\begin{tikzcd}
\operatorname{Hom}(\mathbf{C}^*,H)/W \arrow[r, "\alpha'"] \arrow[d, "\beta'"] & \operatorname{Hom}(\mathbf{C}^*,G)/G \arrow[d, "\beta"] \\
H^1(X,\boldsymbol{O}_X(H))/W \arrow[r, "\alpha"] & H^1(X,\boldsymbol{O}_X(G))
\end{tikzcd}$$

Le théorème 1.1 (resp. 1.2) signifie que α (resp. β) est bijectif. Nous venons de voir que $\operatorname{Hom}(C^*,H) \rightarrow H^1(X,\boldsymbol{O}_X(H))$ donc aussi β' est bijectif, et nous allons démontrer ci-dessous que α' est aussi bijectif. Il en résulte bien que les théorêmes 1.1 et 1.2 sont équivalents. Il reste donc seulement à prouver l'énoncé suivant, sans doute bien connu, de la théorie des groupes de Lie:

Proposition 1.3. *Soit G un groupe de Lie complexe réductif, H un sous-groupe de Cartan, N le normalisateur de H dans G et $W = N/H$ le groupe de Weyl correspondant. Alors tout homomorphisme complexe de $\mathbf{C}^{*n}$ dans G est conjugué par automorphisme intérieur dans G à un homomorphisme complexe de $\mathbf{C}^{*n}$ dans H, qui est unique à une opération de W près.*

Pour montrer que tout homomorphisme u de $A = C^{*n}$ dans G est conjugué à un homomorphisme complexe à valeurs dans H, on peut évidemment supposer G connexe (puisque $u(A) \subset G_0$), et ensuite G semi-simple (puisque H est l'image réciproque d'un sous-groupe de Cartan de G/Z_0, où Z est le centre de G). Alors G peut être regardé comme un groupe algébrique linéaire [3]. Comme toute représentation linéaire holomorphe de A est semi-simple (puisque A est la complexification d'un groupe compact T^n), $u(A)$ est une partie de G formée d'opérateurs semi-simples deux à deux permutables, donc est contenu dans un sous-groupe de Cartan de G [3, Chap. 6, prop. 18], donc, puisque tous les sous-groupes de Cartan de G sont conjugués (loc. cité, th. 4), il existe un $g \in G$ tel que $gu(A)g^{-1} \subset H$, ce qui établit notre assertion. Prouvons maintenant que deux homomorphismes u, u' de A dans H qui sont conjugués dans G, sont conjugués par un élément de N. Il revient au même de dire que si A, B sont deux parties de H et $g \in G$ tels que $gAg^{-1} = B$, alors il existe un $n \in N$ tel que $nan^{-1} = gag^{-1}$ pour tout $a \in A$. (La démonstration très simple qui suit m'a été signalée par A. Borel). Ceci signifie qu'il existe $n \in N$ tel que $m = g^{-1}n$ appartienne au centralisateur M de A. Or $A = g^{-1}Bg$ est contenu dans H et $H' = g^{-1}Hg$, donc M contient H et H', qui sont évidemment encore des sous-groupes de Cartan de M. Il s'ensuit (loc. cité) que l'on peut trouver un $m \in M$ tel que $m^{-1}H'm = H$, et il suffit de poser $n = gm$.

Nous aurons besoin plus bas du résultat suivant, sans doute bien connu; et qui contient prop. 1.3 dans le cas où G est semi-simple connexe:

PROPOSITION 1.4. *Soit G un groupe de Lie complexe connexe semi-simple, H un sous-groupe de Cartan, x et y deux éléments de H tels que pour toute représentation linéaire complexe irreductible de dimension finie U de G, on ait* $\operatorname{Tr} U(x) = \operatorname{Tr} U(y)$. *Alors x et y sont conjugués sous le groupe de Weyl.*

Donnons la démonstration de ce résultat pour la commodité du lecteur. H est une variété algébrique affine (isomorphe à $\mathbf{C}^{*r}$, où r est le rang de G). Soit A l'algèbre des fonctions rationelles sur H, elle s'identifie à l'algèbre du groupe $P^0 \subset \mathfrak{h}'$, réseau du dual $\mathfrak{h}'$ de $\mathfrak{h}$ "polaire" du réseau unité P de $\mathfrak{h}$, à $\lambda \in P^0$ correspondant la fonction $f_\lambda(\exp 2i\pi h) = \exp 2i\pi\langle h, \lambda\rangle$. W est un groupe d'automorphismes de l'algèbre affine A, que peut se définir soit directement à partir des opérations de W sur H, soit par l'intermédiaire des opérations de W sur le groupe P^0. Soit A^W la sous-algèbre des éléments de A invariants sous W, comme W est fini elle "sépare" les trajectoires de W dans H, en d'autres termes deux points x et y de H sont conjugués sous W si et seulement si on a $f(x) = f(y)$ pour toute $f \in A^W$. La proposition sera donc prouvée si nous prouvons que les restrictions à H des caractères des représentations linéaires irréductibles de dimension finie de G engendrent l'espace vectoriel A^W. Or A^W est l'espace vectoriel engendré par les fonctions $\phi_\lambda = \sum_{w \in W} w^*. \ f_\lambda$, où $\lambda \in P^0$. Choisissons une système fondamental de racines relatif à H, alors tout élément de P^0 est transformé par W d'un poids dominant d'une représentation linéaire irréductible de G [2], on peut donc se borner à prendre les λ qui sont de tels poids dominants. Or on voit facilement qu'une telle ϕ_λ est bien combination linéaire à coéfficients entiers de caractères de représentations linéaires irréducibles, grâce au fait que dans la représentation linéaire irréductible de poids dominant donné λ, la multiplicité de λ (donc le coéfficient de f_λ dans l'expression du caractère de la représentation envisagée) est 1.

COROLLAIRE. *Soient* u, u' *deux homomorphismes complexes de* $A = \boldsymbol{C}^{*n}$ *dans* H *tels que pour toute représentation linéaire holomorphe irréducible* U *de dimension finie de* G, *on ait* $\operatorname{Tr} U \circ u = \operatorname{Tr} U \circ u'$. *Alors* u *et* u' *sont conjuguées par une opération du groupe de Weyl.*

Soit T *la circonférence unité dans* $\boldsymbol{C}^*$, soit t un élément de T^n engendrant un sous-groupe dense, il suffit alors d'appliquer la prop. 1.4 à $u(t)$ et $u'(t)$.

Par. 2. Fibrés vectoriels. Nous allons prouver le théorème 1.1 quand G est le groupe linéaire $\boldsymbol{Gl}(r, \boldsymbol{C})$ des automorphismes de l'espace vectoriel complexe $\boldsymbol{C}^r$. Alors la classification des fibrés holomorphes de groupe $\boldsymbol{Gl}(r, \boldsymbol{C})$ est aussi elle des fibrés vectoriels holomorphes. Notons que le sous-groupe H de $\boldsymbol{Gl}(r, \boldsymbol{C})$ formé des matrices diagonales est un sous-groupe de Cartan. Les fibrés holomorphes vectoriels à groupe structural H s'identifient aux fibrés vectoriels E avec une décomposition donnée $E = \sum_{i=1}^{r} E_i$ de E en somme directe de sous-fibrés vectoriels holomorphes à fibre de dimension 1. Le théorême 1.1 s'énonce maintenant ainsi:

THÉORÈME 2.1. *Soit* X *la sphère de Riemann. Tout fibré vectoriel holomorphe* E *sur* X *est somme directe de sous-fibrés vectoriels holomorphes* F_i $(1 \leqq i \leqq r)$ *à fibres de dimension* 1. *Les classes des fibrés* F_i *sont bien déterminées à une permutation près.*

Si on se rappelle que la classe d'un fibré vectoriel holomorphe à fibre $\boldsymbol{C}^*$ est définie par son degré, qui est un entier rationel arbitraire, on obtient le

COROLLAIRE. *L'ensemble* $H^1(X, \boldsymbol{O}_X(\boldsymbol{Gl}(r, \boldsymbol{C})))$ *des classes de fibrés vectoriels holomorphes sur la sphère de Riemann* X, *s'identifie à l'ensemble des suites décroissantes* $n_1 \geqq n_2 \geqq \cdots \geqq n_r$ *de* r *entiers rationnels, a une telle suite correspondant la classe du fibré* $\sum L_{n_i}$, *où* L_n *est le fibré vectoriel holomorphe de fibre* C *sur* X *ayant le degré* n.

La démonstration qui va suivre s'applique aussi bien dans le cadre de la Géométrie Algébrique sur un corps de base algébriquement clos quelconque.

Notons d'abord que d'après Serre [6] la classification des fibrés vectoriels analytiques, ou des fibrés vectoriels algébriques au sens de Weil [8], au dessus d'une variété holomorphe projective (donc algébrique), est la même. Dans le cas où X est une courbe sans singularités, toute application rationelle de X dans une variété projective est régulière (résultat élémentaire purement local) d'où il résulte que plus généralement, toute section rationelle d'un fibré algébrique localement trivial sur X de fibre une variété projective, est en fait régulière. Appliquant ceci au fibré associé au fibré vectoriel algébrique E, de fibré l'espace projectif défini par C^r, on voit qu'on peut trouver un sous-fibré vectoriel algébrique E_1 de E à fibre de dimension 1: il suffit de prendre une section rationelle $s \neq 0$ de E, c'est aussi la section rationelle d'un fibré E_1 du type cherché, évidemment unique. (Le fait que E est un fibré *algébrique* nous sert précisément pour assurer l'existence de sections méromorphes non identiquement nulles!). Appliquant ce résultat au fibré vectoriel E/E_1, on construit de proche en proche une "suite de composition" $E_0 = \{0\} \subset E_1 \subset E_2 \subset \cdots \subset E_r = E$ de E par des sous-fibrés vectoriels holomorphes tels que les E_i/E_{i-1} aient des fibres de dimension 1 $(1 \leqq i \leqq r)$. Soit $d_i = d(E_i/E_{i-1})$ le degré de fibré E_i/E_{i-1}, on va pouver que l'on peut choisir la suite de composition de telle sorte que la suite des d_i soit décroissante.

LEMME 2.2. *Les degrés des sous-fibrés vectoriels holomorphes L de E à fibre de dimension 1 sont bornés supérieurement.*

De façon précise, on a $d(L) \leqq \operatorname{Sup}_i d_i$. En effet, soit i le premier indice tel que $L \subset E_i$, soit $s \neq 0$ une section méromorphe de L, s' la section méromorphe de E_i/E_{i-1} qu'elle définit. Les diviseurs de s et s' satisfont évidemment à $(s) \leqq (s')$, d'où $\deg(s) \leqq \deg(s')$ c'est à dire $d(L) \leqq d(L_i)$, cqfd.

Pour construire maintenant les E_i de façon que la suite d_i soit décroissante, prenons d'abord pour E_1 un sous-fibré vectoriel holomorphe de E, de fibré C, de telle façon que $d(E_1)$ soit le plus grand possible, construisons de même le sous-fibré E_2/E_1 de E/E_1, etc. Je dis que la suite des $d_i = d(E_i/E_{i-1})$ est alors décroissante. On est ramené aussitôt à prouver que $d_2 \leqq d_1$, puis en remplaçant E par E_2, au cas où la fibré de E est de dimension 2. On doit donc prouver:

LEMME 2.3. *Soit E un fibré vectoriel holomorphe de fibre C^2 sur la sphère de Riemann X, soit E_1 un sous-fibré vectoriel holomorphe à fibré C, tel que $d(E_1)$ soit le plus grand possible. Alors $d(E_1) \geqq d(E/E_1)$.*

Nous allons prouver en effet que si $d_1 < d_2$, alors il existe un sous-fibré vectoriel holomorphe de E de degré $> d_1$, c'est à dire qu'il existe une section méromorphe $s \neq 0$ de E telle que $\deg(s) > d_1$. Pour ceci, on peut supposer $d_1 = -1$ d'où $d_2 \geqq 0$, en remplaçant au besoin E par son produit tensoriel avec un fibré vectoriel holomorphe L_{-1-d_1} de degré $-1-d_1$. (En effet, les sous-fibrés vectoriels holomorphes de E et de $L \otimes E$ sont en correspondance biunivoque par $E_1 \rightarrow L \otimes E_1$, et $L \otimes E/E_1$ est isomorphe à $(L \otimes E)/(L \otimes E_1)$, enfin le degré de $L \otimes E_1$ resp. $L \otimes E/E_1$ est égal à celui de E_1 resp. E/E_1 augmenté de $n = -1-d_1$). Pour un fibré vectoriel holomorphe M quelconque, désignons par $\boldsymbol{O}_X(M)$ le faiseau des germes de sections holomorphes de M. On a alors une suite exacte de faisceaux $0 \rightarrow \boldsymbol{O}_X(E_1) \rightarrow \boldsymbol{O}_X(E) \rightarrow \boldsymbol{O}_X(E/E_1) \rightarrow 0$, d'où une suite exacte de cohomologie

$$H^0(X, \boldsymbol{O}_X(E)) \rightarrow H^0(X, \boldsymbol{O}_X(E/E_1)) \rightarrow H^1(X, \boldsymbol{O}_X(E_1)).$$

Or d'après le théorème de dualité [7], $H^1(X, \boldsymbol{O}_X(E_1))$ a même dimension que $H^0(X, \boldsymbol{O}_X(L_{k-d_1}))$ où $k = 2g-2$ est le degré de la "classe canonique" de diviseurs (g désigne le genre de X). Or on a $g = 0$, $d_1 = -1$, d'où $L_{k-d} = L_{-1}$; le diviseur d'une section méromorphe de L_{-1} a pour degré -1, donc ne peut être $\geqq 0$, donc $H^0(X, \boldsymbol{O}_X(L_{-1})) = 0$ et par suite $H^1(X, \boldsymbol{O}_X(E_1)) = 0$, donc la suite exacte précédente prouve que toute section holomorphe de E/E_1 provient d'une section holomorphe de E. Or, comme E/E_1 a un degré $d_2 \geqq 0$, il admet une section holomorphe non nulle, il en est donc de même de E. Une section holomorphe non nulle s de E a un diviseur de degré $\geqq 0$ donc de degré $> d_1 = -1$, ce qui achéve la démonstration du lemme 2. 3.[3]

Soit donc (E_i) une suite de composition du fibré vectoriel E, telle que la suite des degrés d_i des E_i/E_{i-1} $(1 \leqq i \leqq r)$ soit décroissante, nous allons prouver que E est isomorphe à la somme directe des E_i/E_{i-1}. On procède par récurrence sur r, l'assertion étant triviale pour $r = 1$. Supposons la démontrée pour des fibrés vectoriels de fibre $\boldsymbol{C}^{r'}$ avec $r' \leqq r-1$ (r étant un entier $\geqq 2$), prouvons la pour E de fibre $\boldsymbol{C}^r$. D'après l'hypothèse de récurrence, E_{r-1} est isomorphe à $\sum_{i=1}^{r-1} E_i/E_{i-1}$, nous allons prouver que l'extension E du fibré vectoriel $Q = E/E_{r-1}$ par le fibré vectoriel $P = E_{r-1}$ est triviale, c'est à dire qu'il existe un homomorphisme holomorphe de Q dans E qui, composé avec l'homomorphisme canonique $E \rightarrow Q$, donne l'identité. Soit Q'

---

[3] Cette démonstration est due à J. P. Serre. La démonstration originale était beaucoup moins transparente.—Le referee fait remarquer que ce résultat figure aussi, sous une forme différente, dans Atiyah, Proc. L. M. S. 1955.

le fibré dual de Q. La suite exacte $0 \to Q' \otimes P \to Q' \otimes E \to Q' \otimes Q \to 0$ donne naissance à une suite exacte de cohomologie

$$H^0(X, \mathbf{O}_X(Q' \otimes E)) \to H^0(X, \mathbf{O}_X(Q' \otimes Q)) \to H^1(X, \mathbf{O}_X(Q' \otimes P)).$$

Or on a

$$Q' \otimes P \approx \sum_{i=1}^{r-1} (E/E_{r-1})' \otimes (E_i/E_{i-1}) \approx \sum_{i=1}^{r-1} L_{d_i - d_r}$$

d'où $H^1(X, \mathbf{O}_X(Q' \otimes P)) \approx \sum_{i=1}^{r-1} H^1(X, \mathbf{O}_X(L_{d_i-d_r}))$, et comme $d_i - d_r \geqq 0 > -1$, un calcul déjà fait montre que $H^1(X, \mathbf{O}_X(L_{d_i-d_r})) = 0$, d'où $H^1(X, \mathbf{O}_X(Q' \otimes P)) = 0$. Donc le premier homomorphisme de la suite exacte écrite plus haut est surjectif, en particulier l'automorphisme identique de Q (considéré comme section holomorphe du fibré $Q' \otimes Q$) appartient à cette image, i.e., peut se remonter en un homomorphisme holomorphe de Q dans E.[4]

On a démontré la première partie du théorème 2. 1. Reste à prouver que dans une décomposition en somme directe $E = \sum F_i$, les degrés des fibrés F_i de fibré C sont bien déterminés à l'ordre près. Ce fait pourrait se déduire d'un théorème du type Remak-Krull, dû à Atiyah (non publié), affirmant que la décomposition d'un fibré vectoriel holomorphe, sur un espace analytique compact X, en somme directe de fibrés vectoriels "indécomposables," est essentiellement unique. Mais nous aurons besoin dans le cas actuel d'un résultat plus précis, que voici:

PROPOSITION 2. 4. *Soit* $E = \sum_{i=1}^{r} F_i$ *un fibré vectoriel holomorphe sur la sphère de Riemann* X, *somme directe de sous-fibrés vectoriels holomorphes à fibré* $\mathbf{C}$, *de degrés* d_i. *Soit, pour tout entier rationnel* k, E_k *le sous-fibré vectoriel de* E, *somme directe des* F_i *tels que* $d_i \geqq k$. *Alors* E_k *est égal au plus petit sous-fibré vectoriel holomorphe de* E *contenant les sections méromorphes* s *de* E *dont le diviseur est de degré* $\geqq k$ (*en particulier,* E_k *est défini indépendamment de la décomposition donnée de* E).

COROLLAIRE. *Le nombre d'indices* i *tels que* $d_i = k$ *est égal à la dimension de la fibre du fibré vectoriel* E_k/E_{k+1}, *donc ne dépend pas de la décomposition choisie de* E.

La démonstration de la proposition 2. 4 est immédiate, et laissée au lecteur.

---

[4] Nous avons montré que si P et Q sont deux fibrés vectoriels holomorphes sur l'espace analytique X, tels que $H^1(X, \mathbf{O}_X(Q' \otimes P)) = 0$, alors toute extension holomorphe de Q par P est triviale. En fait, il n'est pas difficile de se convaincre que dans tous les cas, les classes d'extensions holomorphes de Q par P correspondent biunivoquement aux éléments de $H^1(X, \mathbf{O}_X(Q' \otimes P))$ (Serre).

Par. 3. Fibrés orthogonaux.

PROPOSITION 3.1. *Soit X un espace analytique compact. L'application canonique de $H^1(X, \boldsymbol{O}_X(\boldsymbol{O}(r, C)))$ dans $H^1(X, \boldsymbol{O}_X(\boldsymbol{Gl}(r, \boldsymbol{C})))$ déduite de l'injection naturelle $\boldsymbol{O}(r, \boldsymbol{C}) \to \boldsymbol{Gl}(r, \boldsymbol{C})$ est injective.*

En d'autres termes, deux fibrés vectoriels orthogonaux holomorphes sur X, isomorphes en tant que fibrés vectoriels holomorphes, sont aussi isomorphes en tant que fibrés vectoriels orthogonaux holomorphes. Pour le prouver, on peut supposer que sur le fibré vectoriel holomorphe E, on a deux structures orthogonales holomorphes définies par la donnée sur toute fibre E_x $(x \in X)$ de deux formes quadratiques (a, b) et $(a, b)_1$ non dégénérées, (fonctions holomorphes du point x), et il faut montrer qu'il existe un automorphisme holomorphe u du fibré vectoriel E, transformant la première forme en la seconde, c'est à dire tel que $(a, b)_1 = (ua, ub)$ pour $a, b \in E_x$. Pour toute fibre E_x, on peut écrire $(a, b)_1 = (A_x a, b)$, où A_x est un endomorphisme de E_x tel que $A = A^*$ (où A^* est l'adjoint de A relativement à la première forme quadratique: $(A^*a, b) = (a, Ab)$ pour $a, b \in E_x$). A_x est inversible, et pour x variable, est une fonction holomorphe de x, donc définit un automorphisme A du fibré vectoriel E. On cherche donc un automorphisme vectoriel holomorphe u de E tel que $(ua, ub) = (Aa, b)$ c'est à dires $A = u^*u$. On va voir qu'on peut même choisir u tel $u = u^*$, et $A = u^*u = u^2$. Pour ceci, considérons le polynôme caractéristique $\det(A - z \cdot 1)$ de A, ses coéfficients sont des fonctions holomorphes sur X, donc constantes puisque X est compacte, pourvu qu'on suppose X connexe, ce qui est loisible. Donc le polynôme caractéristique de A_x est indépendant de x. Soient $\lambda_1, \cdots, \lambda_k$ ses racines distinctes, de multiplicités $\alpha_1, \cdots, \alpha_k$. Pour tout $x \in X$, E_x est somme directe de sous-espaces E^i_x bien déterminés, de dimension α_i, sur chacun desquels A_x induit un opérateur de la form $\lambda_i(\mathbf{1} + u^i_x)$, où u^i_x est nilpotent. Les E^i_x sont orthogonaux deux à deux puisque $A = A^*$. Les E^i_x et les u^i_x sont fonction holomorphes de x, donc E est somme directe de sous-fibrés vectoriels holomorphes E^i $(1 \leqq i \leqq k)$, tels que la fibre de E^i en x soit E^i_x. Soit μ_i une racine carrée de λ_i, posons

$$v^i_x = \mu_i(\mathbf{1} + u^i_x)^{\frac{1}{2}}$$

où on pose $(\mathbf{1} + u^i_x)^{\frac{1}{2}} = \sum_{k=0}^{\alpha_i - 1} (1/k!)\left(\tfrac{1}{2}\right)\left(\tfrac{1}{2} - 1\right) \cdots \left(\tfrac{1}{2} - k + 1\right)(u^i_x)^k$. Alors v^i_x est un endomorphisme de E^i_x fonction holomorphe de x, de plus on a $v^i_x = (v^i_x)^*$. Soit v^i l'endomorphisme de E^i défini par les v^i_x, u leur somme directe, on a $u = u^*$ puisque les v^i sont autoadjoint et les E^i orthogonaux deux à deux, et de plus $u^2 = A$ par construction, ce qui achève la démonstration.

Remarques 1. La démonstration qui précède est encore valable en Géométrie Algébrique sur un corps algébriquement clos quelconque de caractéristique $p \neq 2$. Une démonstration exactement analogue prouverait de même que l'application canonique

$$H^1(X, \boldsymbol{O}_X(\boldsymbol{Sp}(r, \boldsymbol{C}))) \rightarrow H^1(X, \boldsymbol{O}_X(\boldsymbol{Gl}(2r, \boldsymbol{C})))$$

est injective sous les mêmes conditions. On pourrait en déduire directement, comme pour le cas du groupe structural $\boldsymbol{O}(r, \boldsymbol{C})$ traité ci-dessous, la classification des fibrés symplectiques holomorphes sur la sphère de Riemann. Cette démonstration a l'avantage d'être encore directement applicable en Géométrie Algébrique (en caractéristique $p \neq 2$), contrairement à celle du par. 4.

2. L'analogue de la Proposition 3.1 pour le groupe structural $\boldsymbol{SO}(r, \boldsymbol{C})$ au lieu de $\boldsymbol{O}(r, \boldsymbol{C})$ est fausse déjà si $r = 2$ et quand X est la sphère de Riemann.

En vertu de prop. 3.1, la détermination de $H^1(X, \boldsymbol{O}_X(\boldsymbol{O}(r, \boldsymbol{C})))$ revient à la détermination de l'image de cet ensemble dans $H^1(X, \boldsymbol{O}_X(\boldsymbol{Gl}(r, \boldsymbol{C})))$. On a alors:

THÉORÈME 3.2. *Soient X la sphère de Riemann, E un fibré vectoriel holomorphe sur X. Pour qu'il existe sur E une structure orthogonale holomorphe, il faut et il suffit que E soit isomorphe au fibré dual E'. Alors le fibré orthogonal dont il provient est bien déterminé à un isomorphisme près.*

La nécessité de la condition est triviale, et le résultat d'unicité est un cas particulier de prop. 3.1. Reste à prouver que si E est isomorphe à E', E admet une structure orthogonale holomorphe. Mais soit (n_i) la suite des invariants de E (th. 2.1, corollaire) alors la suite des invariants de E' est évidemment à l'ordre près $(-n_i)$, et l'hypothèse signifie que ces deux suites sont les mêmes à une permutation près, c'est à dire que la famille (n_i) est symétrique par rapport à 0. Dans la décomposition $E \approx \sum L_{n_i}$ on peut donc grouper ensemble les composantes qui correspondent à des n_i nuls, et les E_i correspondants à des n_i opposés, donc E apparait comme somme directe d'un fibré trivial E_0, et de fibrés du type $L + L'$. E_0 peut évidemment se munir d'une structure orthogonale, donc le théorème résultera du

LEMME 3.3. *Soit L un fibré vectoriel holomorphe sur un espace ana-*

lytique X, soit L' son dual. Alors le fibré $L + L'$ est muni d'une structure orthogonale canonique.

Il suffit en effet, sur chaque fibré $L_x + L'_x$, d'introduire la forme bilinéaire symétrique

$$(a + a', b + b') = \langle a, b' \rangle + \langle b, a' \rangle$$

où les produits scalaires du second membres sont relatifs à l'accouplement naturel de L_x et de son dual.

Proposition 3.4. *Soient X la sphère de Riemann, E un fibré vectoriel orthogonal sur X, et soit pour tout entier rationnel k, E_k le plus petit sous-fibré vectoriel holomorphe de E contenant les sections méromorphes ayant un diviseur de degré $\geqq k$* (*cf. prop.* 2.4). *Alors le sous-fibré vectoriel de E orthogonal de E_k est E_{-k+1}.*

Par raison de symétrie, on peut supposer $k \geqq 1$. D'après le théorème 3.2, E est de la forme

$$E = E_0 + \sum_{n_i > 0} (L_{n_i} + L_{-n_i})$$

où les facteurs E_0 et $(L_{n_i} + L_{-n_i})$ sont deux à deux orthogonaux, enfin les L_{n_i} et L_{-n_i} isotropes et E_0 constant. La proposition résults alors immédiatement de la prop. 2.4.

Par. 4. Démonstration du théorème principal. a) *Reduction du group structural.*

Lemme 4.1. *Soient X un espace analytique complexe compact, G un groupe de Lie complexe, P un fibré holomorphe sur X de groupe structural G, E le fibré associé adjoint de fibre l'algèbre de Lie $\mathfrak{G}$ de G (où G opère par la représentation adjointe). Supposons qu'on connaisse une section holomorphe s de E tellé que, en au moins un point $a \in X$, $s(a)$ soit un élément régulier* [3, Chap. 6] *de l'algèbre de Lie E_a, fibre de E en a. Alors $s(x)$ est un élément régulier de E_x pour tout $x \in X$.*

Les coéfficients $a_i(s(x))$ du polynôme caractéristique de $\operatorname{ad} s(x)$ sont des fonctions holomorphes sur X, donc constantes puisque X est compact. Or dire que $s(x)$ est régulier signifie que $a_r(s(x)) \neq 0$, où r est le rang de $\mathfrak{G}$. D'où la conclusion.

Corollaire 1. *Sous les conditions précédentes, on peut réduire le groupe structural G de P au normalisateur N d'un sous-groupe de Cartan H de G.*

En effet, soit pour tout $x \in X$, $\mathfrak{h}(x)$ la sous-algèbre de E_x centralisateur de $s(x)$. C'est une sous-algèbre de Cartan puisque x est régulier, et elle est fonction holomorphe de x comme on le vérifie sans difficulté. Soit $\mathfrak{h}$ une sous-algèbre de Cartan de $\mathfrak{G}$, H le sous-groupe de Cartan correspondent de G. Le normalisateur N de H est aussi identique à l'ensemble des $g \in G$ qui invarient $\mathfrak{h}$ dans la représentation adjointe de G. Donc l'espace homogène G/N est isomorphe à l'espace des sous-algèbres de Cartan de $\mathfrak{G}$ (se rappeler que deux sous-algèbres de Cartan sont toujours conjugées!) et le fibré associé à P et de fibre G/N est celui dont la fibre, en un point $x \in X$, est l'ensemble des sous-algèbres de Cartan de l'algèbre de Lie E_x. Or nous avons construit une section holomorphe $x \to \mathfrak{h}(x)$ de ce fibré, ou ce qui revient au même, nous avons réduit à N le groupe structural de P, ce qui prouve le corollaire.

COROLLAIRE 2. *Si de plus X est simplement connexe, on peut réduire le groupe structural au sous-groupe de Cartan H.*

En effet, N/H est discret, donc le fibré de fibre N/H associé à un fibré holomorphe de groupe N est trivial puisque X est simplement connexe, donc le groupe structural peut se réduire à H.

Nous supposons maintenant que X est la sphère de Riemann, et allons montrer que si G est un groupe de Lie holomorphe *réductif*, la condition du lemme 4.1 est automatique satisfaite, c'est à dire qu'on peut trouver une section holomorphe s de E telle que $s(a)$ soit un élément régulier de E_a pour au moins un $a \in X$. On a $\mathfrak{G} = \mathfrak{Z} + \mathfrak{G}'$ où $\mathfrak{Z}$ est le centre et $\mathfrak{G}'$ l'algèbre dérivée de $\mathfrak{G}$, et cette décomposition est invariante sous la représentation adjointe de G. Il en résulte une décomposition analogue de E en somme directe de deux sous-fibrés dont la fibre en chaque point x est le centre resp. l'algèbre dérivée de l'algèbre E_x. Comme un élément régulier de l'algèbre dérivée de E_x est régulier dans E_x, on voit aussitôt, en envisageant le fibré de fibre $\mathfrak{G}'$, de groupe $\operatorname{Aut}\mathfrak{G}'$ associé au fibré P et à la représentation de G dans $\operatorname{Aut}\mathfrak{G}'$ déduite de la représentation adjointe, qu'on peut se ramener au cas où G est un groupe semi-simple (savoir $\operatorname{Aut}\mathfrak{G}'$), ce que nous supposerons désormais.

Soit alors E_k le sous-fibré vectoriel de E engendré par les sections méromorphes dont le diviseur est de degré $\geqq k$ (cf. prop. 2.4). On vérifie aussitôt que $[E_k, E_{k'}] \subset E_{k+k'}$ car si s, s' sont deux sections méromorphes de E, le degré $\deg([s, s'])$ du diviseur de la section $[s(t), s'(t)]$ est manifestement $\geqq \deg(s) + \deg(s')$, car $([s, s']) \geqq (s) + (s')$. Il en resulte en particulier que E_1 est un fibré de *sous-algèbres* de Lie de E, et que si $\mathfrak{G}_1$ est la fibre de E_1 en un point fixé $a \in X$, et si on identifie $\mathfrak{G}$ à la fibre E_a, alors pour $Y \in \mathfrak{G}_1$, $\mathrm{ad}_{\mathfrak{G}} Y$ est *nilpotent*. D'autre part, E est en fait un fibré orthogonal (grâce à la forme de Killing sur $\mathfrak{G}$, invariante par automorphismes) et nous avons vu (corollaire au th. 3.2) que l'orthogonal de E_1 est forcément E_0. Soit $\mathfrak{G}_0$ la fibre de E_0 en a, c'est donc l'orthogonal de $\mathfrak{G}_1$ dans $\mathfrak{G}$ pour la forme de Killing. Or on a:

LEMME 4.2. *Soient $\mathfrak{G}$ une algèbre de Lie complexe semi-simple, $\mathfrak{G}_1$ une sous-algèbre telle que pour tout $X \in \mathfrak{G}_1$, $\mathrm{ad}_{\mathfrak{G}} X$ soit nilpotent. Par suite $\mathfrak{G}_1$ est nilpotent et à fortiori contenue dans une sous-algèbre résoluble maximale $\mathfrak{R}$ de $\mathfrak{G}$. Alors $\mathfrak{R}$ est contenue dans l'orthogonal $\mathfrak{G}_0$ de $\mathfrak{G}_1$ (pour la forme de Killing).*

En effet, on sait qu'on a $\mathfrak{R} = \mathfrak{h} + \mathfrak{N}$, où $\mathfrak{h}$ est une sous-algèbre de Cartan, et $\mathfrak{N} = \mathfrak{R}'$ est le plus grand idéal nilpotent de $\mathfrak{R}$. Il s'ensuit que tout élément X de $\mathfrak{R}$ tel que $\mathrm{ad}_{\mathfrak{G}} X$ soit nilpotent est dans $\mathfrak{N}$ (il suffit même que $\mathrm{ad}_{\mathfrak{R}} X$ soit nilpotent!) en particulier $\mathfrak{G}_1 \subset \mathfrak{N}$. D'autre part, il est bien connu aussi que $\mathfrak{R}$ est orthogonal à $\mathfrak{N}$, donc à fortiori à $\mathfrak{G}_1$, donc contenu dans $\mathfrak{G}_0$. Le lemme 4.2 est démontré. Comme il existe des éléments réguliers dans $\mathfrak{h}$, on obtient le

COROLLAIRE. *Sous les conditions précédentes, il existe un élément régulier de $\mathfrak{G}$ contenu dans $\mathfrak{G}_0$.*

Revenons alors à notre démonstration. D'après sa définition et prop. 2.4, E_0 est isomorphe à une somme directe de fibrés vectoriels holomorphes de fibre $\boldsymbol{C}$, de degrés $\geqq 0$, d'où résulte aussitôt que pour tout élément u de la fibré $\mathfrak{G}_0$ de E_0 en a, il existe une section holomorphe s de E_0 prenant la valeur u en a. D'après le corollaire précédent, on peut choisir u régulier. Cela prouve que la condition du lemme 4.1 est bien satisfaite. En vertu du corollaire 2 dudit lemme, nous voyons que le groupe structural de P peut se réduire à H, ce qui démontre la première moitié du théorème principal 1.1: l'application (1) du par. 1 est surjective. Reste à prouver qu'elle est injective.

b) *Résultat d'unicité à une opération de W près.* Dans ce qui suit, X sera toujours la sphère de Riemann. Supposons d'abord G semi-simple connexe. Soit ξ un élément de $H^1(X, \boldsymbol{O}_X(H))$, ξ_1 son image dans $H^1(X, \boldsymbol{O}_X(G))$. On a vu au par. 1 que ξ est la classe du fibré associé au fibré L_1 (de groupe $\boldsymbol{C}^*$) et à un homomorphisme complexe u de $\boldsymbol{C}^*$ dans H bien déterminé. Nous allons montrer comment la connaissance de ξ_1 détermine u à une opération de W près. Pour toute représentation linéaire complexe de G, on a une application naturelle

$$H^1(X, \mathbf{O}_X(G)) \xrightarrow{u^*} H^1(X, \mathbf{O}_X(\mathbf{Gl}(r, \mathbf{C})))$$

(r étant le degré de la représentation), en faisant correspondre à un fibré holomorphe de groupe G le fibré vectoriel associé (pour la représentation U). Ce dernier est aussi associé à L_1 et la représentation linéaire $U \circ u$ de $\mathbf{C}^*$, donc la classe du fibré vectoriel associé à L_1 et $U \circ u$ est connue quand on connait ξ_1. D'après le théorème 1, 2, déjà démontré (sous la forme équivalente 1. 1) au par. 2 dans le cas du groupe linéaire général, on en conclut que $U \circ u$ est connu à une similitude près, à fortiori la fonction $\operatorname{Tr} U(u(t))$ sur $\mathbf{C}^*$ est connue. Ceci étant vrai pour toute représentation linéaire U de dimension finie de G, on peut en conclure, en vertu de prop. 1. 4, corollaire, que u lui-même est déterminé à une opération de W près.

Supposons maintenant G réductif et connexe.

LEMME 4. 3. *Soit G un groupe de Lie complexe réductif connexe. Alors il existe un sous-groupe fini z du centre de G tel que G/z soit isomorphe au produit d'un groupe abélien par un groupe semi-simple.*

Le groupe de revêtement universel de G est isomorphe à un produit $V \times F$, où V est un espace vectoriel complexe et F un groupe semi-simple complexe. G est donc isomorphe au quotient de $V \times F$ par un sous groupe discret Γ du centre de $V \times F$. Ce centre est identique à $V \times \pi$, où π est le centre de F, donc fini en vertu d'un théorème fondamental de H. Weyl [2]. Il en résulte que la projection L de Γ sur V est un sous-groupe *fermé* de V, de *même rang* que Γ, donc Γ est un sous-groupe d'indice fini de $L \times \pi$. Posant maintenant $z = (L \times \pi)/\Gamma$, le lemme 4. 3 est démontré.

Le théorème 1. 1 étant vrai si G est semi-simple connexe comme on a vu plus haut, ou si G est abélien connexe comme on a vu au par. 1, il s'ensuit aussitôt qu'il est encore vrai pour le produit de deux tels groupes, donc pour le group G/z du lemme 4. 3. Notons que H/z est un sous-groupe de Cartan de G/z et N/z son normalisateur. Considérons le diagramme commutatif d'applications naturelles:

$$\begin{tikzcd}
H^1(X, \mathbf{O}_X(H)) \arrow[r] \arrow[d] & H^1(X, \mathbf{O}_X(G)) \arrow[d] \\
H^1(X, \mathbf{O}_X(H/z)) \arrow[r] & H^1(X, \mathbf{O}_X(G/z)) .
\end{tikzcd}$$

Soient ξ, ξ' deux éléments de $H^1(X, \mathbf{O}_X(H))$ ayant même image dans

$H^1(X, \mathbf{O}_X(G))$, alors leurs images ξ_1, ξ'_1 dans $H^1(X, \mathbf{O}_X(H/z))$ ont même image dans $H^1(X, \mathbf{O}_X(G/z))$, donc d'après ce qu'on a dit, sont conjugués sous le groupe de Weyl $(N/z)/(H/z)$ de G/z, qui est isomorphe au groupes de Weyl $W = N/H$ de G. Par suite ξ et ξ' sont conjugués sous W mod un élément du noyau de l'homomorphisme $H^1(X, \mathbf{O}_X(H)) \to H^1(X, \mathbf{O}_X(H/z))$. Or ce noyau est nul, en vertu de la suite exacte de cohomologie déduite de la suite exacte $0 \to z \to H \to H/z \to 0$, puisque $H^1(X, z) = 0$ (X étant simplement connexe). Cela démontre le th. 1.1 dans le cas où G est connexe.

Supposons enfin G réductif quelconque. Soient ξ, ξ' deux éléments de $H^1(X, \mathbf{O}_X(H))$ ayant même image dans $H^1(X, \mathbf{O}_X(G))$. Soient ξ_1, ξ'_1 leurs images dans $H^1(X, \mathbf{O}_X(G_0))$, ξ_1 et ξ'_1 ont même image dans $H^1(X, \mathbf{O}_X(G))$, et sont par suite conjugués par une opération du groupe $H^0(X, \mathbf{O}_X(G/G_0)) = G/G_0$ (en vertu par exemple de la "suite exacte de cohomologie" pour les faisceaux non commutatifs, développée dans [4]). Un élément de G/G_0 opère sur $H^1(X, \mathbf{O}_X(G_0))$ en prenant un représentant $g \in G$ et considérant l'automorphisme $g_0 \to g g_0 g^{-1}$ de G_0. Or il existe un représentant qui est dans N, comme on a vu à la fin de la démonstration de prop. 1.3. On en conclut qu'en remplaçant ξ' par un conjugué de ξ' sous W, on peut supposer que $\xi_1 = \xi'_1$. D'après le théorème 1.1 pour G_0, on en conclut que ξ et ξ' sont conjugués sous le groupe de Weyl de G_0 et à fortiori sous W, ce qui achève la démonstration.

Remarques finales. 1. On peut se demander si le th. 1.1 ou le th. 1.2 reste valable pour *tout* groupe structural de Lie complexe G. On s'aperçoit qu'il est déjà en défaut quand G est le groupe des transformations affines $z \to az + b$ (a, b complexes). On notera cependant que la technique de "dévissage" exposée dans [4], jointe aux résultats de ce travail, permettent en principe de déterminer $H^1(X, \mathbf{O}_X(G))$ pour tout groupe G donné. Je ne connais toutesfois pas de description simple de $H^1(X, \mathbf{O}_X(G))$ en termes de théorie des groupes de Lie complexes.

2. Il semble plausible que la seule variété projective X sur laquelle tout fibré vectoriel holomorphe soit décomposable en somme de fibrés holomorphes de fibre $\mathbf{C}$, soit la sphère de Riemann. On note en tous cas que si X est une courbe algébrique projective non singulière de genre $g \neq 0$, i.e. telle que $H^1(X, \mathbf{O}_X) \neq 0$, il existe sur X un fibré vectoriel holomorphe *indécomposable* à fibre $\mathbf{C}^2$: si E_0 est le fibré vectoriel constant de fibre $\mathbf{C}$, il suffit de prendre un fibré E extension non triviale[4] de E_0 par E_0. E est indécomposable, car s'il était décomposé en la somme de deux fibrés E_1, E_2

de fibre C, on conclurait d'abord que chaque E_i admet une section holomorphe non nulle (puisque E en admet une engendrant un sous-fibré qui n'est pas "facteur direct") donc a un degré $\geqq 0$; comme la somme de ses degrés est identique à $\deg(E) = \deg(E_0) + \deg(E_0) = 0$, ils doivent être nuls, ce qui, joint à l'existence d'un section holomorphe, implique que E_i est constant, donc E est constant; mais alors toute section holomorphe de E est constante, donc si elle est $\neq 0$, la structure d'extension qu'elle définit sur E est triviale, contrairement à la construction de E comme extension non triviale. Notons encore que si X est l'espace projectif complexe P^n de dimension $n \geqq 2$, alors le fibré tangent n'est pas même réductible à la forme triangulaire; autrement, le fibré dual E le serait aussi, d'où on conclurait aisément que $H^i(X, \boldsymbol{O}_X(E)) = 0$ pour $i \neq 0, n$ (car on sait que pour tout fibré vectoriel holomorphe L de fibré $\boldsymbol{C}$ sur $X = P^n$, on a $H^i(X, \boldsymbol{O}_X(L)) = 0$ si $i \neq 0, n$ [5, Chap. 3, prop. 8]); or $\boldsymbol{O}_X(E)$ est le faisceau Ω^1 des germes de 1-formes différentielles holomorphes, et $H^1(X, \Omega^1) = H^{1,1}(X, \boldsymbol{C})$ (cohomologie de type $(1, 1)$ de X); mais il est bien connu que $H^{1,1}(X, \boldsymbol{C}) \neq 0$ pour toute variété projective sans singularités X de dimension complexe $\geqq 1$. Pour finir, prenons pour X la "variété des drapeaux" sur P^2 (isomorphe canoniquement à la variété des drapeaux dans l'espace vectoriel $\boldsymbol{C}^3$), c'est donc un espace fibré algébrique sur P^2 de fibre $P^1 =$ sphère de Riemann. Le fibré tangent de la base P^2 n'est pas réductible à la forme triangulaire, mais son image réciproque E sur X l'est évidemment, E est cependant, indécomposable, comme il résulte du fait plus général suivant: Soit p une application holomorphe d'un espace analytique X sur un autre Y, identifiant Y à un "espace analytique quotient" de X, i.e. telle que les fonctions holomorphes f sur un ouvert U de Y soient celles telles que $f \circ p$ soit holomorphe sur $p^{-1}(U)$. Supposons que pour tout $y \in Y$, $p^{-1}(y)$ soit compact et connexe. Soit E un fibré vectoriel holomorphe sur Y; *pour que E soit indécomposable, il faut et il suffit que $p^{-1}(E)$ le soit.* De façon plus précise, les décompositions de E en somme directe de deux sous-fibrés vectoriels holomorphes correspondent biunivoquement aux decompositions analogues de $p^{-1}(E)$. Elles s'identifient en effet aux systêmes de deux projecteurs complémentaires de l'algèbre $H^0(Y, \boldsymbol{O}_Y(E' \otimes E))$ (E' désignant le fibré dual de E), tandis que les décompositions de $p^{-1}(E)$ s'identifient aux systêmes de deux projecteurs complémentaires dans l'algèbre $H^0(X, \boldsymbol{O}_X(p^{-1}(E' \otimes \mathrm{E})))$, et il suffit de montrer que si (f_1, f_2) est un tel systême, alors chaque section f_i provient d'une section holomorphe de $E' \otimes E$ sur Y, ou encore (en vertu de l'hypothèse sur p) que sa restriction aux "fibres" $p^{-1}(y)$ sont des sections *constantes*. Or, ceci résulte du fait que $p^{-1}(E' \otimes E)$ induit un fibré constant sur chaque fibre, et de l'hypothèse faite sur les fibres.[5]

UNIVERSITY OF KANSAS AND
CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE.

REFERENCES.

[1] H. Cartan, *Séminaire E. N. S.*, 1953-1954.

[2] P. Cartier, *Séminaire Sophus Lie*, 1. ère année (1954-1955).

[3] C. Chevalley, *Théorie des Groupes de Lie III*, Paris (1955).

[4] A. Grothendieck, *A General Theory of Fibre Spaces with Structure Sheaf*, University of Kansas (1955).

[5] J. P. Serre, "Faisceaux Algébriques Cohérents," *Annals of Mathematics*, vol. 61 (1955), pp. 197-278.

[6] ———, Géometrie Algébrique et Géométrie Analytique, Annales de l'Inst. Fourier, vol. 6 (1955-56), pp. 1-42.

[7] ———, "Un Théorême de Dualité," *Comm. Math. Helvet.*, vol. 29 (1955), pp. 9-26.

[8] A. Weil, *Fibre Spaces in Algebraic Geometry* (Notes by A. Wallace), Chicago University, 1952.

---

[5] Comme me l'a fait observer le referee, la condition que la fibre soit connexe (et que j'avais malencontreusement omise) est essentielle pour la validaté du résultat indiqué, un contre-exemple dans le cas contraire étant obtenu ainsi: on prend $X = Y =$ courbe elliptique, $p(x) = 2x$ (au sens de la loi du groupe), de sorte que X devient un révêtement à 4 feuillets de Y, et on prend pour E un fibré extension non triviale du fibré en droites défini par le diviseur (P) (P un point de Y) par le fibré en droites trivial. (Le fait que $p^{-1}(E)$ est décomposable peut être prouvé à l'aide des résultats de Atiyah, Proc. London Math. Soc. 1955).

BOUNDED MATRICES AND LINEAR DIFFERENTIAL EQUATIONS.*

By Aurel Wintner.

The following considerations deal with ordinary (homogeneous) linear differential equations in Hilbert space, with coefficient matrices which are bounded. It is well-known that the choice of bounded "matrices," instead of bounded "operators," is not a loss of generality. Some of the results to be obtained seem to be new in the case of finite matrices also.

1. Let $x_1, x_2, \cdots$ be complex numbers, $x = (x_1, x_2, \cdots)$ a vector in Hilbert's space ($|x| < \infty$), every capital $C, F, \cdots$ a bounded matrix, $|C|$ the least upper bound of the length $|Cx|$ of the vector Cx when $|x| = 1$ (so that $|C| < \infty$), and C° the (bounded, Hermitian) matrix $\frac{1}{2}(C + C^{*})$. If $C(x, y)$ denotes the bilinear form determined by C, then the real part of the value of the form $C(x, \bar{x})$ is identical with that of the Hermitian form $C^{\circ}(x, \bar{x})$, since, if C_0 is defined by $C = C^{\circ} + C_0$, then $C_0{}^{*} = -C_0$, hence $\operatorname{Re} C_0(x, \bar{x}) = 0$. Clearly, $C = C^{\circ}$ if and only if C is Hermitian. It also follows from

$$\operatorname{Re} C(x, \bar{x}) = C^{\circ}(x, \bar{x}) \tag{1}$$

that if λ denotes the least, and μ the greatest, value occurring in the spectrum of the Hermitian matrix C°, then, since λ is known to be the greatest lower, and μ the least upper, bound of $C^{\circ}(x, \bar{x})$ for $|x| = 1$,

$$\lambda |x|^2 \leqq \operatorname{Re} C(x, \bar{x}) \leqq \mu |x|^2. \tag{2}$$

The (finite, non-negative) difference $\mu - \lambda$, *the real spectral span of* C, will be denoted by $[C]$; so that

$$[C] = \underset{|x|=1}{\text{l. u. b.}} \operatorname{Re} C(x, \bar{x}) - \underset{|x|=1}{\text{g. l. b.}} \operatorname{Re} C(x, \bar{x}), \tag{3}$$

hence

$$[C] = [C^{\circ}], \text{ where } C^{\circ} = \tfrac{1}{2}(C + C^{*}). \tag{3 bis}$$

C is called non-singular if there exists a *unique* bounded C^{-1} satisfying $CC^{-1} = I$ and/or $C^{-1}C = I$, where I is the unit matrix.

---

* Received October 31, 1956.

2. If there is given a bounded matrix $C = C(t)$ at every point t of an interval $0 \leqq t < \omega$, where $\omega \leqq \infty$, and if $|C(t_n) - C(t)| \rightarrow 0$ as $n \rightarrow \infty$ holds for every fixed t whenever $t_n \rightarrow t$, then $C(t)$ will be called continuous. Starting with such a $C(t)$ and denoting dx/dt by x', consider for the vector $x = x(t)$ the differential equation

$$x' = C(t)x \tag{4}$$

with an initial condition $x(0)$ satisfying $|x(0)| < \infty$. It is well-known (cf. [5], p. 1477, or [3], pp. 681-684, where further references are given) that this initial value problem has a unique solution $x = x(t)$, satisfying $|x(t)| < \infty$, on the entire interval $0 \leqq t < \omega$. The proof of these assertions is word by word the same as in the case of the finite-dimensional case, since both the customary existence proofs, such as that based on successive approximations, and the uniqueness argument of Lipschitz are applicable without any change.

What is somewhat less straightforward is the transfer to the case of Hilbert's space of the main theorem on the "fundamental matrices" $X(t)$ of (1), since, in the finite-dimensional case, the proof of that theorem is usually based on the identity

$$d(t) = d(0) \exp \int_0^t \operatorname{tr} C(s)\, ds, \text{ where } d(t) = \det X(t), \tag{5}$$

(Jacobi-Liouville), an identity which is not available in the general case. For a simple argument replacing the use of (5), cf. Section 4 below.

3. A vector $x(t)$ will not be considered a solution of (4) unless $|x(t)| < \infty$ for $0 \leqq t < \omega$. This implies that $|x(t)| > 0$ throughout unless $x(t)$ is the trivial solution, $x(t) \equiv 0$. In fact, if $0 \leqq t_0 < \omega$, then $x(t) \equiv 0$ is a solution of (4) satisfying the initial condition $x(t_0) = 0$, and so the assertion follows from the uniqueness theorem. Let $x(t)$ be any solution of (4) distinct from the trivial solution; so that

$$0 < r(t) < \infty \text{ for } 0 \leqq t < \omega, \text{ where } r = \tfrac{1}{2}|x|^2. \tag{6}$$

Under the assumption that $C = C(t)$ is continuous for $0 \leqq t < \omega$, let $\lambda = \lambda(t)$ and $\mu = \mu(t)$, where t is fixed, be the least and greatest values occurring in the spectrum of the Hermitian matrix $C^0 = C^0(t)$, where $C^0 = \frac{1}{2}(C + C^*)$. Then multiplication of (4) and of the complex conjugate of (4) by $\bar{x}=\bar{x}(t)$ and $x=x(t)$ respectively, when followed by an application of (1) and (2), shows that

$$(7) \qquad 2\lambda(t)r(t) \leqq r'(t) \leqq 2\mu(t)r(t) \quad \text{for } 0 \leqq t < \omega,$$

by (6). Since $r'(t)/r(t)$ is the derivative of $\log r(t)$, it is clear from (6) and (7) that

$$(8) \qquad |x(0)| \exp \int_0^t \lambda(s)ds \leqq |x(t)| \leqq |x(0)| \exp \int_0^t \mu(s)ds,$$

where $0 \leqq t < \omega$, holds for the length of every solution $x(t)$ of (4).

In [16], pp. 558-559, this inequality was derived, for a certain asymptotic purpose, in the finite-dimensional case (for later references, cf. [2], pp. 20-22, or [17], Section 2). But the proof has nothing to do with this restriction and, although both the proof and the assertion of (8) are simple indeed, the central position of (8) in the theory of (4) has not been noted in the literature. It will be seen that the consequences of (8) are manifold.

The simplest consequence of (8) results if (8) is applied to the case $C(t) =$ const. of (4). Then (8) reduces to an inequaliy deduced by Heinz [4], pp. 426-427, by arguments which are applicable in the particular case $C(t) =$ const.; cf. Section 5 below.

4. Let $X(t)$ denote a matrix of the form $(x^1(t), \cdots, x^m(t), \cdots)$ in which every column vector $x^m(t)$ is a solution $x(t)$ of (4). If the initial data $x^1(0), \cdots, x^m(0), \cdots$ are so chosen that $X(0)$ is a bounded matrix, then $X(t)$ will be called a solution matrix of (4). If, in addition, $X(0)$ is chosen to be non-singular (cf. the end of Section 1), then $X(t)$ will be called a fundamental matrix of (4). It will be concluded from (8) that if t is fixed on the interval $0 < t < \omega$, then the matrix $X(t)$ is (a) a bounded matrix for every solution matrix and (b) a non-singular matrix in case of a fundamental matrix. Assertion (b) is the fact which, in the finite-dimensional case, is usually concluded from (5).

With reference to a fixed m, let $X_m(t)$ denote the solution matrix corresponding to which the k-th column of $X_m(0)$ is the vector 0 or the k-th column of the unit matrix I according as $m < k < \infty$ or $1 \leqq k \leqq m$. Then, if the definition of $|C|$ (cf. the first sentence of Section 1) is applied to $C = X_m(t)$, it is readily seen from (8) that, in view of the superposition principle of (4), both inequalities

$$(9) \qquad \exp \int_0^t \lambda(s)\,ds \leqq |X(t)| \leqq \exp \int_0^t \mu(s)\,ds, \text{ where } 0 \leqq t < \omega,$$

hold for $X(t) = X_m(t)$. Hence, if $m \to \infty$, and if $X(t)$ now denotes the fundamental matrix determined by the initial condition

$$(10) \qquad X(0) = I,$$

then (9) holds for this $X(t)$ also. In particular, the second of the inequalities (9) shows that this $X(t)$ is a bounded matrix for every non-negative $t < \omega$. But it also follows from (10) that the solution $x(t)$ of (4) belonging to an arbitrary initial vector $x(0)$ (with $|x(0)| < \infty$) is

$$(10\,\text{bis}) \qquad x(t) = X(t)x(0), \text{ where } 0 \leqq t < \omega,$$

and that, correspondingly, the most general solution matrix [fundamental matrix] of (4) is $X(t)A$, where $A = \text{const.}$ is an arbitrary [non-singular] bounded matrix.

This, when combined with the relations $|B_1B_2| \leqq |B_1||B_2|$ and $|I| = 1$ (and with the choice $B_1 = B$, $B_2 = B^{-1}$ when B is non-singular), proves both of the assertions (a)-(b). In fact, (a) follows in a refined form, according to which

$$(11) \qquad |X(t)| \leqq |X(0)| \exp \int_0^t \mu(s)\,ds, \text{ where } 0 \leqq t < \omega,$$

holds for every solution matrix $X(t)$, and (b) follows in a refined form, acocrding to which

$$(12) \qquad |X^{-1}(t)| \leqq |X^{-1}(0)| \exp \int_0^t -\lambda(s)\,ds, \text{ where } 0 \leqq t < \omega,$$

holds for every fundamental matrix.

5. The simplest corollary of (11) is the inequality of Heinz, referred to at the end of Section 3. It states that, if A is any bounded matrix,

$$(13) \qquad |e^A| \leqq \exp \underset{|x|=1}{\text{l. u. b.}}\, A^0(x, \bar{x}), \text{ where } A^0 = \tfrac{1}{2}(A + A^*)$$

(e^A is defined by $I + \cdots + A^n/n! + \cdots$). In fact, if the numbers λ, μ denote the best bounds satisfying the case $C = A$ of (2) (for every x), then (13) is equivalent to the first of the two inequalities

$$(14) \qquad |e^A| \leqq e^{\mu}, \qquad |e^{-A}| \leqq e^{-\lambda}.$$

If the coefficient matrix $C(t)$ of (4) is chosen to be the given bounded $A = \text{const.}$ (the t-interval can be chosen to be the half-line $0 \leqq t < \infty$), then the fundamental matrix $X(t)$ belonging to (10) is $X(t) = e^{tA}$. Hence, if λ, μ are the constants defined before (14), then (11) and (12) reduce to $|e^{tA}| \leqq e^{\mu t}$ and $|(e^{tA})^{-1}| \leqq e^{-\lambda t}$, and so (14) follows by choosing $t = 1$.

6. It is possible to reduce the second of the inequalities (14) to the first, which is (13) (cf. Heinz, [4], pp. 426-428, and the end of Section 8 below). In any case, both parts of (14) are involved in the following estimate, which will be needed below: If T is a non-singular matrix of the form e^A, where A is bounded matrix, and if F is any bounded matrix, then

$$(15) \qquad |TFT^{-1}| \leqq e^{[A]}|F|, \text{ where } T = e^A$$

Here $[A]$ denotes the "real spectral span" of A, as defined in Section 1. Hence $e^{[A]} = e^{\mu-\lambda}$ in the notations used in (14). Thus it is clear from $|B_1B_2B_3| \leqq |B_1||B_2||B_3|$ that (15) follows from (14).

7. As proved in [14] (in this connection, cf. [13], pp. 281-282, and the end of p. 267), there belongs to every bounded, non-singular T a unique unitary $U = (U^*)^{-1}$ and a unique (bounded) positive definite $P = P^*$ satisfying $T = PU$. It turns out that, in terms of the $P = P_T$ of T, it is possible to formulate the estimate (5) of the *affine distortion* of a bounded matrix F in such a way as to dispose of the hypothesis implicit in (15), viz., of the restriction that T, besides being non-singular, be such as to possess a bounded logarithm $(= A)$ or, what is the same thing, that T be embeddable (as T^1) into a continuous cyclic semi-group of bounded matrices T^t, where $0 \leqq t < \infty$.

The resulting generalization of (15) is as follows: If T and F are bounded, and if T is non-singular, then

$$(16) \qquad |TFT^{-1}| \leqq [P]|F|,$$

where $[P]$ is the (real) spectral span of the positive definite factor $P = P^*$ in $T = PU$.

First, as pointed out in [13], p. 267, there belongs to every bounded, positive definite $P = P^*$ a unique bounded $Q = Q^*$ satisfying $P = e^Q$, and the spectrum of this Q consists of the (real) logarithms of the values occurring in the spectrum of P. In particular, $[P] = e^{[Q]}$. Hence the assertion (16), where $T = PU$, is equivalent to

$$(16\text{ bis}) \qquad |e^QUFU^{-1}e^{-Q}| \leqq e^{[Q]}|F|.$$

But the truth of (16 bis) follows from the case $T = e^Q$ of (15), since, U being unitary, $|UFU^{-1}| = |F|$.

8. If H is bounded and Hermitian, then the same is true of e^H, and e^H is positive definite, since, in view of the spectral resolution of H, a value a is in the spectrum of H if and only if e^a is in the spectrum of e^H (and since, every a being real, every e^a is positive). Similarly, e^{iH} is a unitary matrix and, as first proved in [13], pp. 268-277, every unitary matrix can be represented in the form e^{iH}.

If A is bounded, then there exists a unique pair of bounded Hermitian matrices H, K satisfying $A = H + iK$; in fact, $H = A^0$, $K = A_0$ in the notations of Section 1. Let e^H and e^{iK} be denoted by P and U respectively. Then $PU = UP = e^A$ if $HK = KH$ (that is, if A is normal). In this case and, more generally, if $e^{H+iK} = PU$ happens to be true, it is clear from $|B_1B_2| \leqq |B_1||B_2|$ and $|U| = 1$ that $|e^A| \leqq |P|$.

It turns out, however, that the last inequality is true for *every* bounded A; in other words, *if A is bounded, and if $H = H^*$ and $K = K^*$ are defined by $A = H + iK$, then $|e^{H+iK}| \leqq e^H$.* In fact, since e^H is positive definite (cf. the beginning of this Section 8), there exists a unique (bounded) positive definite Q satisfying $e^H = e^Q$ (cf. Section 7), and so the last italicized statement is equivalent to the first of the relations (14), where $A = K + iH$. The second of the relations (14) follows if A is replaced by $-A$ in the last italicized assertion.

9. In what follows, the asymptotic behavior (as $t \to \infty$) of the solution vectors (xt) of (4) will be considered, when appropriate restrictions are placed on the behavior of the coefficient matrix $C(t)$. *It will always be assumed that $0 \leqq t < \infty$, and that the matrix $C(t)$ is bounded and continuous for fixed t* (but neither $|C(t)| <$ const. as $t \to \infty$ nor the uniform continuity of $C(t)$ for $0 \leqq t < \infty$ will be assumed).

(i) *In terms of a given $C = C(t)$, where $0 \leqq t < \infty$, define $C^0 = C^0(t)$ by $C^0 = \frac{1}{2}(C + C^*)$ (so that $(C^0)^* = C^0$), and $\lambda = \lambda(t)$, $\mu = \mu(t)$ by placing*

$$\lambda = \underset{|x|=1}{\text{g.l.b.}}\, C^0(x, \bar{x}), \qquad \mu = \underset{|x|=1}{\text{l.u.b.}}\, C^0(x, \bar{x}) \tag{17}$$

(for fixed t). Suppose that both integrals

$$\int_0^\infty \lambda(t)\,dt, \quad \int_0^\infty \mu(t)\,dt, \quad \text{where } \int_0^\infty = \lim_{t\to\infty} \int_0^t, \tag{18}$$

are convergent (both $\int^{\infty} |\lambda(t)|\, dt = \infty$ *and* $\int^{\infty} |\mu(t)|\, dt = \infty$ *are allowed). Then the length* $|x(t)|$ *of every solution vector* $x(t) \not\equiv 0$ *of* (4) *tends to a finite and non-vanishing limit as* $t \to \infty$.

This follows by replacing $s = 0$ and $s = t$ in (8) by $s = u$ and $s = v$ respectively, and then letting $v - u \to \infty$.

(ii) *If* $C(t)$ *satisfies the assumptions of* (i), *then there belongs to every fundamental matrix* $X(t)$ *of* (4) *a pair of constants satisfying* $|X(t)| <$ const. *and* $|X^{-1}(t)| <$ Const. *as* $t \to \infty$.

This is clear from (11) and (12).

(iii) *The assumptions imposed on* $C(t)$ *in* (i) *and* (ii) *are satisfied if (but not only if)*

$$\int_0^{\infty} |C^{\circ}(t)|\, dt < \infty, \text{ where } C^{\circ} = \tfrac{1}{2}(C + C^{*}). \tag{19}$$

In fact, (19) is sufficient for the *absolute* convergence of the integrals (18), since it follows from (17) that $|\lambda| \leqq |C^{\circ}|$, $|\mu| \leqq |C^{\circ}|$.

10. The assumption (19) puts no restriction on the "skew-symmetric" component of C; that is, on the matrix which, in Section 1, was denoted by C_0. Correspondingly,

$$\int_0^{\infty} |C(t)|\, dt < \infty \tag{20}$$

is an assumption which is even stricter than (19). It turns out that, if (20) is assumed, then much more than what is assured by (i) and (ii) can be asserted:

(iv) *If the coefficient matrix* $C(t)$ *of* (4) *satisfies* (20), *then*

$$X(t) \to I \text{ as } t \to \infty \tag{21}$$

holds for a certain (unique) fundamental matrix $X(t)$ *of* (4).

In the case of finite matrices, the assertion of (iv) is well-known; it goes back to Bôcher and Dunkel (cf. their papers, referred to in the first two footnotes in [7], p. 486, to which I called attention some time ago). The following proof is so primitive as to hold for bounded matrices also.

Let $X(t)$ be any fundamental matrix of (4). Then, since (20) is sufficient for (19), it follows from (iii) that (ii) is applicable. But since (4) is equivalent to $X'(t)=C(t)X(t)$, it follows from (20) and from the first of the assertions of (ii) that, since $|CX|\leqq|C||X|$,

$$\int_0^\infty |X'(t)|\,dt<\infty\text{; in particular, }\int_0^\infty X'(t)dt=\lim_{s\to\infty}\int_0^s dX(t)$$

is convergent; that is, $X(\infty)=\lim X(s)$, where $s\to\infty$, exists in the weak sense, to begin with. But the first assertion of (ii) assures that $X(\infty)$ is a bounded matrix, and the second assertion of (ii) shows that $X(\infty)$ is non-singular. Hence, it is sufficient to replace the given fundamental matrix $X(t)$ by $X(t)X^{-1}(\infty)$ in order to obtain the fundamental matrix satisfying (21).

11. By Lagrange's device of the variation of constants (in this regard, cf. [15], pp. 190-191), the following criterion on "small perturbations" can now be concluded:

(v) *For every fixed t, where* $0\leqq t<\infty$, *let* $C(t)$ *and* $B(t)$ *be bounded and continuous. Suppose that, for large t, the matrix* $C(t)-B(t)$ *is so "small" with reference to a fundamental matrix* $X(t)$ *of* $x'=C(t)x$ *that*

$$\int_0^\infty |G(t)|\,dt<\infty,\text{ where } G=X^{-1}(C-B)X. \tag{22}$$

Then $y'=B(t)y$ *possesses a fundamental matrix* $Y(t)$ *of the form*

$$Y(t)=X(t)(I+Z(t)),\text{ where }\lim_{t\to\infty}|Z(t)|=0. \tag{23}$$

Due to (iv), the proof of (v) is the same as the proof given in [15], pp. 200-201 (where the matrices are finite), and can therefore be omitted.

12. If (v) is combined with (15), then there results an asymptotic statement which seems to be new even in case of finite matrices. In fact, a result of [15], pp. 188-196 (1946) and the similar, but less inclusive, results of Erugin (1946; cf. [11], pp. 176-182), apply, in case of finite matrices, in the same direction as (vi) below but are weaker than what (vi) becomes in the case of finite matrices.

(vi) *Let* $[A]$ *denote the real spectral span of a bounded matrix* $A=$ const. *and let* $F(t)$, *where* $0\leqq t<\infty$, *be a matrix which, for every fixed t, is bounded and continuous. Suppose that*

(24) $$\int_0^\infty e^{[A]t} \, | F(t) | \, dt < \infty$$

(*where* $|F| = \text{l.u.b.} \, |Fx|$ *for* $|x| = 1$). *Then the case* $C(t) = A + F(t)$ *of* (4) *possesses a fundamental matrix* $X(t)$ *of the form*

(25) $$X(t) = e^{tA}(I + Z(t)), \text{ where} \lim_{t \to \infty} | Z(t) | = 0.$$

In order to prove this, let the A and $F(t)$ in (vi) be identified with the $C(t)$ and $B(t)$ of (v) respectively. The $Y(t)$ of (v) becomes the $X(t)$ of (vi), and the $X(t)$ of (v) can be chosen to be e^{tA}, since e^{tA} is a fundamental matrix of the case $C(t) = A$ of (4). Accordingly, (23) and (22) go over into (25) and

(26) $$\int_0^\infty | e^{-tA} F(t) e^{tA} | \, dt < \infty$$

respectively. Consequently, (vi) follows from (v) if it is ascertained (24) is sufficient for (26). But it is clear from (3) that $|tA| = |t| A$. Hence, the sufficiency of (24) for (26) follows if A is replaced by $-tA$ in (15).

13. Let $\lambda = \text{const.}$ be the greatest lower bound of (1) for $|x| = 1$, where $C = \text{Const.}$ is any bounded matrix. Then Satz 6 of Heinz ([4], p. 428; cf. [10], passim) states that if $\lambda > 0$, then C is non-singular and, in addition,

(27) $$C^{-1} = \int_0^\infty e^{-tC} \, dt$$

and $|C^{-1}| \leqq \lambda^{-1}$. Heinz points out that the first of these assertions, that preceding (27), is a refinement of a result of Toeplitz, and he mentions certain recent references concerning this refinement. But neither [4] nor [10] mentions that this (viz., the existence of a unique, bounded C^{-1} if $\lambda > 0$) is contained, in a substantially improved form, in the results of [13], and that, corresponding to this improvement, (27) can be improved to the following assertion: *If A is bounded, then the Liouville-Neumann expansion*

(28) $$(zI - A)^{-1} = \sum_{n=0}^{\infty} z^{-n-1} A^n$$

(which is certainly valid, in the sense of convergence, outside the circle $|z| \leqq |A|$) *is valid, in the sense of (absolute) Borel summability, outside the least convex region containing those complex numbers z for which $zI - A$ is non-singular*; cf. Section 15 below.

What is today generally called the spectrum of an arbitrary bounded C was first defined in [13], p. 239, as the set $\sigma(C)$ of those complex numbers z for which $zI - C$ fails to be non-singular. It was proved in [13], pp. 242-243, that $\sigma(C)$ is a closed bounded set which contains at least one point. There is a curious oversight in [12], p. 149 (repeated in [10], pp. 409-412 and disguised in [8]): both the definition of $\sigma(C)$ and the proof for the existence of $\sigma(C)$ are *verbatim* the same in [13].

Let $\rho(C)$ denote the closure of the set of the (complex) values attained by the bounded form $C(x, \bar{x})$ when $|x| = 1$. For finite matrices C, it was conjectured by Toeplitz, and proved by Hausdorff, that

(29) $\rho(C)$ is convex,

and it was proved by Toeplitz that

(30) $\sigma(C)$ is a subset of $\rho(C)$.

When Toeplitz proved (30) for finite matrices, the definition of $\sigma(C)$ for bounded matrices was not in the literature, and if it would have been, his proof, having been based on eigenvectors, could not have led to (30) for bounded C. But it was shown in [13], p. 245, that the definition of $\sigma(C)$, introduced in [13], p. 239, is such as to lead to the truth of (30) for any bounded C. In contrast, the truth of (30) for every bounded C was clear from the beginning, since it is implied by the truth of (30) for every finite C; cf. [13], p. 244.

14. If H is a bounded Hermitian matrix, then $\sigma(H)$ is a bounded set of real numbers which, in view of (29), is an interval and about which the spectral resolution of H impiles that $\rho(H)$ is the *least* interval containing $\sigma(H)$ (cf. [13], p. 250; this cannot be concluded from (30) alone).

If this is applied to $H = C^\circ$, then it is clear from (29), (30) and (1) that $z = 0$ cannot be in $\sigma(C)$ if it is not in $\rho(C^\circ)$. This means that C must be non-singular if C° is positive definite (or negative definite), that is, if $\lambda > 0$ (or $\mu < 0$) in (17). This is the result quoted before (28).

15. Let $\tau(C)$ denote the convex closure of $\sigma(C)$. Then it is clear from (30) and (29) that

(31) $\tau(C)$ is a subset of $\rho(C)$.

The fact referred to at the beginning of Section 14 is equivalent to the statement that (31) can be replaced by

$$(32) \qquad \tau(H) = \rho(H) \text{ if } H = H^*$$

(the same holds for normal matrices; cf. [13], p. 282.)

The result of Heinz, quoted in connection with (27), states that if λ is the least value occurring in the set (32) when $H = C^\circ$, then $\lambda > 0$ implies that C is non-singular, that (27) holds, and that $| C^{-1} | \leqq 1/\lambda$. Hence, if C is replaced by $zI - C$, and if λ_z denotes the least value occurring in the set (32) when $H = (zI - C)^\circ$, then $\lambda_z > 0$ implies that $z = 0$ is not in $\tau(C)$, that

$$(33) \qquad (zI - C)^{-1} = \int_0^\infty e^{-t(zI-C)}\, dt,$$

and that

$$(34) \qquad |(zI - C)^{-1}| \leqq 1/\lambda_z.$$

Thus, if C is replaced by $e^{i\phi}C$, where ϕ is an arbitrary real scalar, then, by comparing the supporting function of the convex set $\tau(C)$ with the supporting function of Borel's convex "indicatrix" (of a power series of non-vanishing radius of convergence; cf. [1], pp. 120-129; [9], pp. 578-593), it is readily found that (28) is valid, in the sense of Borel's (absolute) summation process, precisely on the z-domain which is the complement of the (closed, bounded) set $\tau(C)$. In fact, $(zI - C)^{-1}$ is a "(bounded) regular function" on the complement of $\sigma(C)$. For, on the one hand, $\tau(C)$ contains $\sigma(C)$ and, on the other hand, $(zI - C)^{-1}$ can be expanded, in a sufficiently small circle $| z - z_0 | < \gamma = \gamma(z_0)$, into a "(bounded) regular power series" in $z - z_0$, if z_0 is any point in the complement of $\tau(C)$; cf. [13], p. 242 and pp. 245-247.

It should be emphasized that, in view of (31), the Borel summability in $z - z_0$, if z_0 is any point in the complement of $\sigma(C)$; cf. [13], p. 242 and be concluded from, the Borel summability of (28) on the complement of $\rho(C)$.

Appendix.

Let a bounded A be called logarithmizable, or an l-matrix, if there exists some bounded C for which $A = e^C$ holds. Every l-matrix is non-singular (in fact, $Be^C = I$ and $e^CB = I$ are satisfied by the bounded matrix $B = e^{-C}$). Around 1929 I raised the question whether the converse is also true (as it is in case of finite matrices, in which case the customary proofs depend on the theory of elementary divisors or, at least, on the theorem of Hamilton-Cayley; cf. however [19], p. 364). Now it is finally sure that the answer is in the negative:

In order that a bounded matrix be logarithmizable, it is (necessary but) not sufficient that it be non-singular.

In fact, it is clear (cf. the end of p. 361 in [19]) that an A cannot be an l-matrix unless there exists some bounded B satisfying $A = B^2$. But it was recently shown by Halmos, Lumer and Schäffer [18] that for certain (bounded) non-singular A there will not exist such a B.

Accordingly, the l-matrices form a *proper* subset of the group of all non-singular matrices. Is this subset a group? The answer to this question, too, proves to be negative:

The logarithmizable matrices fail to form a group.

In fact, it was proved in [13], pp. 268-277 and p. 267, that every unitary U and every positive definite (non-singular) $P = P^*$ is an l-matrix. On the other hand, as shown in [14], every non-singular A has a unique factorization of the form $A = PU$. Hence, if the product of two l-matrices were always an l-matrix, it would follow that every non-singular A is an l-matrix.

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] E. Borel, *Leçons sur les séries divergentes,* Paris, 1901.

[2] R. Conti, "Sulla stabilità dei sistemi di equazioni differenziali lineari," *Rivista di Matematica della Università di Parma,* vol. 6 (1955), pp. 3-34.

[3] H. Hamburger, "Zur Theorie der sphärischen Abbildung im Grossen. I," *Mathematische Zeitschrift,* vol. 31 (1930), pp. 629-708.

[4] E. Heinz, "Beiträge zur Störungstheorie der Spektralzerlegung," *Mathematische Annalen,* vol. 123 (1951), pp. 415-438.

[5] E. Hellinger and O. Toeplitz, "Grundlagen für eine Theorie der unendlichen Matrizen," *Mathematische Annalen,* vol. 69 (1910), pp. 289-330.

[6] ———, Article II Cl. 13 (1927) in the Encyclopädie der mathematischen Wissenschaften, vol. II, part 3_2.

[7] E. Hilb, Article II B 5 (1913) in the Encyclopädie der mathematischen Wissenschaften, vol. II, part 2.

[8] J. von Neumann, " Eine Spektraltheorie für allgemeine Operatoren eines unitären Raumes," *Mathematische Nachrichten*, vol. 4 (1951), pp. 258-281.

[9] G. Pólya, " Untersuchungen über Lücken und Singularitäten von Potenzreihen," *Mathematische Zeitschrift*, vol. 29 (1929), pp. 549-640.

[10] F. Riesz and B. Sz.-Nagy, *Leçons d'analyse fonctionnelle*, third edition, Paris, Budapest, 1955.

[11] V. V. Stepanoff and V. V. Nemitsky, *Qualitative theory of differential equations* (in Russian), Moscow, 1949.

[12] M. H. Stone, *Linear Transformations in Hilbert Space*, New York, 1932.

[13] A. Wintner, " Zur Theorie der beschränkten Bilinearformen," *Mathematische Zeitschrift*, vol. 30 (1929), pp. 228-289.

[14] ———, " On non-singular bounded matrices," *American Journal of Mathematics*, vol. 54 (1932), pp. 142-149.

[15] ———, " Linear variations of constants," *ibid.*, vol. 68 (1946), pp. 185-213.

[16] ———, "Asymptotic integration constants," *ibid.*, vol. 68 (1946), pp. 553-559.

[17] ———, " Energy dissipation and linear stability," *Quarterly of Applied Mathematics*, to appear.

APPENDIX.

[18] P. Halmos, G. Lumer, and J. J. Schäffer, " Square roots of operators," *Proceedings of the American Mathematical Society*, vol. 4 (1953), pp. 142-149; cf. P. Halmos and G. Lumer, Part II, *ibid.*, vol. 5 (1954), pp. 589-595.

[19] A. Wintner, " On the logarithms of bounded matrices," *American Journal of Mathematics*, vol. 74 (1952), pp. 360-364.

A NOTE ON ENTROPY.*

By I. I. Hirschman, Jr.[1]

Let $\|f\| = (\int_{-\infty}^{\infty} |f(x)|^2 dx)^{\frac{1}{2}}$, where $f(x) \in L^2(-\infty, \infty)$ and let

$$f(x) \sim \int_{-\infty}^{\infty} g(y) e^{2\pi i x y} dy, \qquad g(y) \sim \int_{-\infty}^{\infty} f(x) e^{-2\pi i x y} dx, \tag{1}$$

where the $\sim$ refers to convergence in the mean of L^2 (*Plancherel*); so that $\|f\| = \|g\|$. If

$$\|f\| = \|g\| = 1, \tag{2}$$

then $|f(x)|^2$ and $|g(y)|^2$ may be considered as probability frequency functions. The variance $V[\phi]$ of a frequency function is defined by

$$V[\phi] = \int_{-\infty}^{\infty} (x - m)^2 \phi(x) dx, \text{ where } m = \int_{-\infty}^{\infty} x\phi(x) dx$$

is the mean value. $V[\phi]$ may be taken as a measure of the "concentration" of ϕ in the neighborhood of its mean, a small value of V corresponding to a high degree of concentration. Weyl, [4], has shown that not both of the frequency functions $|f(x)|^2$ and $|g(y)|^2$ can be highly concentrated in this sense and that in fact

$$V[|f(x)|^2] V[|g(y)|^2] \geqq 1/16\pi^2,$$

a relation having application to the uncertainty principle of quantum mechanics.

In this note we shall demonstrate a similar result concerning entropy. The entropy $E[\phi]$ of a frequency function $\phi(x)$ is

$$E[\phi] = \int_{-\infty}^{\infty} \phi(x) \log \phi(x) dx.$$

Entropy is a measure of concentration of ϕ on a set of small measure, a large positive value of E corresponding to a high degree of concentration.

---

* Received August 16, 1956.

[1] This research was supported in part by the Office of Scientific Research and Development Command of the United States Air Force under contract.

We shall show that in the sense of entropy $|f(x)|^2$ and $|g(y)|^2$ cannot both be highly concentrated. More precisely we shall prove the following result.

THEOREM. *Under the assumptions* (1) *and* (2),

$$E[|f(x)|^2]+E[|g(y)|^2]\leqq 0 \tag{3}$$

whenever the left hand side has meaning.

There are heuristic arguments which suggest that the extremal functions in the inequality (3) are $f(x)=\pi^{-\frac{1}{4}}e^{-x^2/2}$ and its dilations. Consequently our theorem may hold with the improved conclusion

$$E[|f(x)|^2]+E[|g(y)|^2]\leqq \log 2-1. \tag{4}$$

However I have not been able to establish this. If this inequality is valid in this form then it includes the inequality of Weyl since for any frequency function $\phi(x)$ we have

$$E[\phi]\geqq -\tfrac{1}{2}-\tfrac{1}{2}\log\{2\pi V[\phi]\}. \tag{5}$$

See [2]. More generally if

$$M_{a,p}[\phi]=[\int_{-\infty}^{\infty}|x-a|^p\phi(x)\,dx]^{1/p} \qquad (-\infty<a<\infty, 0<p<\infty),$$

then the argument used to prove (5) shows that

$$E[\phi]\geqq -\log A(p)-\log M_{a,p}[\phi], \text{ where } A(p)=2p^{(1-p)/p}e^{1/p}\Gamma(1/p).$$

Using (3) we find that for $0<p<\infty$, $0<q<\infty$,

$$M_{a,p}[|f(x)|^2]M_{b,q}[|g(y)|^2]\geqq 1/A(p)A(q).$$

However the inequalities obtained, even if (4) is used in place of (3), are clearly not best possible except when $p=q=2$.

For further studies of the "concentration" of pairs of Fourier transforms, see the paper of W. H. Fuchs [1].

We now turn to the demonstration of Theorem 1. Let us agree that $E[|f(x)|^2]$ is defined whenever one of the integrals

$$\int_{-\infty}^{\infty}|f(x)|^2\log^+|f(x)|^2\,dx, \qquad \int_{-\infty}^{\infty}|f(x)|^2\log^-|f(x)|^2\,dx$$

is finite. The left hand side of (3) therefore has meaning except in the following two cases: a. one of $E[|f(x)|^2]$ or $E[|g(y)|^2]$ is undefined; b. one of $E[|f(x)|^2]$ and $E[|g(y)|^2]$ is $+\infty$ and the other $-\infty$.

Our demonstration consists in subjecting the integral form of the Young-Hausdorff inequality, see [5], to that limit process which leads from the powers of a positive number to its logarithm. We begin by supposing that $f(x) \in L^1(-\infty, \infty) \cap L^2(-\infty, \infty)$. Let $p^{-1} + q^{-1} = 1$. We set

$$C(p) = q^{-1} \log[\int_{-\infty}^{\infty} |g(y)|^q \, dy] - p^{-1} \log[\int_{-\infty}^{\infty} |f(x)|^p \, dx].$$

By the Young-Hausdorff theorem (the extension to Fourier transforms is due to Titchmarsh), $C(p) \leqq 0$, if $1 < p \leqq 2$. Parseval's equality gives $C(2) = 0$, and these together show that $C'(2-) \geqq 0$, if, of course, $C'(2-)$ exists.

For each x the function

$$[|f(x)|^2 - |f(x)|^p]/(2-p) \tag{6}$$

increases to $|f(x)|^2 \log |f(x)|$ as $p \uparrow 2-$. Since the function (6) is integrable for any fixed $p < 2$ it follows that

$$\text{if } A(p) = \int_{-\infty}^{\infty} |f(x)|^p \, dx, \text{ then } A'(2-) = \int_{-\infty}^{\infty} |f(x)|^2 \log |f(x)| \, dx,$$

where $A'(2-)$ is always defined, $-\infty < A'(2-) \leqq +\infty$. Similarly,

$$\text{if } B(q) = \int_{-\infty}^{\infty} |g(y)|^q \, dy, \text{ then } B'(2+) = \int_{-\infty}^{\infty} |g(y)|^2 \log |g(y)| \, dy,$$

where $B'(2+)$ is always defined, $-\infty \leqq B'(2) < +\infty$.

From $C(p) = q^{-1} \log B(q) - p^{-1} \log A(p)$, $(p^{-1} + q^{-1} = 1)$,

$$C'(2-) = -\tfrac{1}{2} B'(2+) - \tfrac{1}{2} A'(2-). \tag{7}$$

Here we have used $B(2) = A(2) = 1$. The relation (7) in conjunction with the inequality $C'(2-) \geqq 0$ shows that (3) holds except in the case when $E[f] = +\infty$ and $E[g] = -\infty$.

If it is no longer assumed that the quantities

$$\| f \|^2 = \int_{-\infty}^{\infty} |f(x)|^2 \, dx = \int_{-\infty}^{\infty} |g(y)|^2 = \| g(y) \|^2$$

are 1 then our relation becomes

$$E[|f|^2] \| f \|^{-2} + E[|g|^2] \| g \|^{-2} \leqq \log \| f \|^2 + \log \| g \|^2. \tag{8}$$

We now abandon our assumption that $f(x) \in L^1(-\infty, \infty)$. It is sufficient to consider the case when $E[|f|^2]$ and $E[|g|^2]$ are defined. Let $\omega_T(x)$ be $1 - |x| T^{-1}$ for $|x| \leqq T$ and 0 for $|x| > T$, and let $\Omega_T(y)$

$=\sin^2 \pi Ty/(\pi^2 Ty^2)$ be the Fourier transform of $\omega_T(x)$. The functions $\omega_T(x)f(x)$ and $\Omega_T(y)*g(y)$ are Fourier transforms of each other and $\| \omega_T(x)f(x) \| = \| \Omega_T(y)*g(y) \| \leqq 1$. Since $\omega_T(x)f(x) \in L^1(-\infty, \infty)$ we may apply (10) to conclude that either

$$E[| \omega_T(x)f(x) |^2] + E[\Omega_T(y)*g(y) |^2] \leqq 0 \tag{9}$$

holds or $E[| \omega_T f |^2] = +\infty$ and $E[| \Omega_T * g |^2] = -\infty$.

A simple application of the Lebesgue limit theorem gives $\lim_{T\to\infty} E[| \omega_T f |^2] = E[| f |^2]$. The functions

$$\theta_1(z) = | z |^2 \log^+ | z |, \qquad \theta_2(z) = | z |^2[-\log^- | z | + \tfrac{3}{2}]$$

are convex in the complex variable z. Since $\Omega_T(y) \geqq 0$ $(-\infty < y < \infty)$ and $\int_{-\infty}^{\infty} \Omega_T(y)\,dy = 1$, it follows that for $i = 1, 2$

$$\lim_{T\to\infty} \int_{-\infty}^{\infty} \theta_i[\Omega_T(y)*g(y)]\,dy = \int_{-\infty}^{\infty} \theta_i[g(y)]\,dy.$$

Since $E[| g |^2] = 2 \int_{-\infty}^{\infty} \theta_1(g)\,dy - 2 \int_{-\infty}^{\infty} \theta_2(g)\,dy + 3 \| g \|^2$, we have

$$\lim_{T\to\infty} E[| \Omega_T(y)*g(y) |^2] = E[| g |^2].$$

The inequality (3) now follows from (9).

Let G be an arbitrary locally compact Abelian group with elements $x, y, \cdots$ and let $G^\wedge$ be its dual with elements $x^\wedge, y^\wedge, \cdots$. Let dx and $dx^\wedge$ be Haar measures on G and $G^\wedge$ so normalized that

$$\text{if } f^\wedge(x^\wedge) \sim \int_G f(x)\,\overline{(x, x^\wedge)}\,dx, \text{ then } f(x) \sim \int_{G^\wedge} f^\wedge(x^\wedge)\,(x, x^\wedge)\,dx^\wedge.$$

Under these assumptions Parseval's equality,

$$\| f(x) \|^2 = \int_G | f(x) |^2\,dx = \int_{G^\wedge} | f^\wedge(x^\wedge) |^2\,dx^\wedge = \| f^\wedge(x^\wedge) \|^2,$$

holds; see [3]. The argument leading to (3) can easily be extended to show that if $\| f \| = \| f^\wedge \| = 1$, then

$$E[| f |^2] + E[| f^\wedge |^2] \leqq 0, \tag{10}$$

where

$$E[| f |^2] = \int_G | f(x) |^2 \log | f(x) |^2\,dx,$$

$$E[| f^\wedge |^2] = \int_{G^\wedge} | f^\wedge(x^\wedge) |^2 \log | f^\wedge(x^\wedge) |^2\,dx^\wedge.$$

In particular if $f(\theta) \sim \sum_{-\infty}^{\infty} a_n e^{2\pi i n\theta}$, $a_n = \int_0^1 f(\theta) e^{-2\pi i n\theta} d\theta$, and

$$\sum_{-\infty}^{\infty} | a_n |^2 = \int_0^1 | f(\theta) |^2 d\theta = 1,$$

then

$$\sum_{-\infty}^{\infty} | a_n |^2 \log | a_n |^2 + \int_0^1 | f(\theta) |^2 \log | f(\theta) |^2 d\theta \leqq 0. \tag{11}$$

If $f(\theta) = 1$, so that $a_0 = 1$, $a_n = 0$ for $n \neq 0$, then equality obtains in (11); consequently the number 0 on the right hand side of (11) cannot be replaced by a smaller value. This also shows that (10) cannot be improved for the class of "all" locally compact Abelian groups. However it is conceivable that for individual groups the right hand side of (10) can be replaced by a smaller value. In particular this would seem to be the case when G is the real line which is the case we have treated in detail.

WASHINGTON UNIVERSITY.

REFERENCES.

[1] W. H. Fuchs, "On the magnitude of Fourier transforms," *Proc. Inter. Congress of Mathematicians at Amsterdam*, 1954, vol. 2, pp. 106-107.

[2] C. Shannon and W. Weaver, *A Mathematical Theory of Communication*, Urbana, 1949.

[3] A. Weil, *Intégration dans les groupes topologiques et ses applications*, Paris, 1940.

[4] H. Weyl, *Group Theory and Quantum Mechanics* (English translation), New York, 1931.

[5] A. Zygmund, *Trigonometrical Series*, Lwów, 1935.

INTEGRAL EQUIVALENCE OF QUADRATIC FORMS IN RAMIFIED LOCAL FIELDS.*

By O. T. O'Meara.

Two quadratic forms with associated matrices F and G are said to be integrally equivalent if there exists a unimodular matrix X such that $X^TFX = G$. Is it possible to attach a set of invariants to F which will completely characterize the equivalence class F, i.e., such that F and G will be integrally equivalent if and only if they have the same invariants? An answer to this problem has been given by Durfee [DI] in the case where the coefficients are taken in a local field in which 2 is a unit; Jones [JI] and Pall [PI] have established similar results over the 2-adic numbers. In an earlier paper [OI] I provided a characterization that holds for any local field in which 2 is a prime, and I discussed the equivalence of unitary forms in the ramified extensions of the 2-adic numbers. It is the purpose of this paper to solve the remaining case in the local theory—the equivalence of forms with coefficients in a field in which 2 is not a unit.

We shall consistently use the language of vector spaces and lattices when framing definitions and proving theorems. The invariants will be given in terms of fundamental invariants a_j, $v(j)$ which describe the numbers represented by certain invariant substructures of a given lattice. Using these quantities, the equivalence class of a lattice will be determined by Hasse symbols and quadratic residues.

Proofs will be based on the results of [OI], and no attempt will be made to give a self-contained discussion here. However, using the principles of the present paper it is possible to improve some of the earlier proofs and I have thought it worth while to include a simplified treatment of the invariance of type. Theorem 5.2 of [OII] will also be proved agan; but for this result, the present paper is independent of [OII].

I want to express my appreciation and indebtedness to Professor G. Whaples for making several valuable suggestions that have simplified the presentation of these results.

Notation. We preserve the notation used in [OI]. Thus our coefficient field F will be a local field [AI] with ring of integers $\mathfrak{o}$; π will denote a

---

* Received September 26, 1955; revised August 22, 1956.

prime element in F; throughout this paper we will assume that the residue class field is perfect, thought not necessarily finite, and that $\infty > e = \operatorname{ord} 2 \geqq 1$. We will continue to use the following notation: $\alpha\pi^t$ will sometimes be written $[\pi^t]$ if α is a unit and $\{\pi^t\}$ is α is an integer. The relation $\alpha \cong \beta$ means that there is a unit in F whose square is α/β. If ϵ is a unit, then $\epsilon \cong 1 \bmod \pi$ follows immediately from the perfectness of the residue class field. Consider the greatest value of k for which $\epsilon \cong 1 + [\pi^k]$. If $k > 2e$, then $k = \infty$ by Hensel's lemma. On the other hand, we can again use the perfectness of the residue class field to prove that

$$(1) \qquad k < 2e \implies k \text{ odd}.$$

We define $\mathfrak{g}(\epsilon)$ as the ideal $\pi^k\mathfrak{o} + 2\mathfrak{o}$ where k is the maximal value just mentioned. For any $\epsilon\pi^r \in F$ we put

$$(2) \quad \mathfrak{g}(\epsilon\pi^r) = \mathfrak{g}(\epsilon) = \pi^k\mathfrak{o} + 2\mathfrak{o} \text{ if } r \text{ is even, } \mathfrak{g}(\epsilon\pi^r) = \mathfrak{o} \text{ if } r \text{ is odd, } \mathfrak{g}(0) = 0.$$

V will denote an n-dimensional vector space over F, provided with scalar product $x \cdot y$. It is assumed that V is non-degenerate, in other words

$$x \cdot y = 0 \text{ for all } y \in V \implies x = 0.$$

By a lattice L on V we mean an $\mathfrak{o}$-module $L \subseteq V$ which contains n independent vectors and is such that if the variable vector $x \in L$ is expressed in a fixed basis for V, then the coordinates of x in this basis have bounded denominators. It is well-known that a minimal basis $\langle x \rangle$ can be found such that $L = \sum \mathfrak{o}x_\lambda$. For a proof see Satz 1 [AsI]. Using this minimal basis it is easy to see that corresponding to any $x \in V$, there exists an $\alpha \in F$ such that $\alpha x \in L$, $\alpha\pi^{-1}x \notin L$; if $x \notin L$, then α must be in $\pi\mathfrak{o}$; otherwise $|\alpha| \geqq 1$. We shall refer to a subset $L' \subseteq V$ as a lattice in V if L' is a lattice on its containing space FL'.

Now let L and K be two lattices on V and suppose that they are expressed in the bases $L = \sum \mathfrak{o}x_\lambda$ and $K = \sum \mathfrak{o}y_\lambda$ respectively. We have seen in [OI] that L is isometric to K (written $L \cong K$) if and only if the matrices $(x_i \cdot x_j)$ and $(y_i \cdot y_j)$ are integrally equivalent. If l is the quadratic form associated with $(x_i \cdot x_j)$, we write $L \cong (x_i \cdot x_j) \cong l$. We recall that $N(L) = \sum \mathfrak{o}x^2$ where x runs through L; and $d(L) = \det(x_i \cdot x_j)$. Then the assumption that V is non-degenrate is equivalent to $d(L) \neq 0$.

We will write $x \cdot L$ to denote $\{(x \cdot y) \mid y \in L\}$, where x is an arbitrary vector in V. More generally, we put

$$L \cdot K = \{(x \cdot y) \mid x \in L, y \in K\},$$

for any lattices L and K in V. It is easy to see that $x \cdot L$ is an $\mathfrak{o}$-ideal in F. This is also true for $L \cdot K$. For let $\langle z \rangle$ be an orthogonal basis for V. Since the elements of L and K have bounded denominators in $\langle z \rangle$, we can suppose that $L \subseteq \sum \mathfrak{o} z_\lambda$ and $K \subseteq \sum \mathfrak{o} z_\lambda$. Hence $L \cdot K$ generates a finite ideal $\pi^k \mathfrak{o}$, say. Suppose that $|x_0 \cdot y_0| = |\pi^k|$. Then $\mathfrak{o} x_0 \cdot y_0 = \pi^k \mathfrak{o}$. Hence $L \cdot K = \pi^k \mathfrak{o}$. And so $L \cdot K$ is an $\mathfrak{o}$-ideal in F. The lattice L is said to be integral if $N(L) \subseteq \mathfrak{o}$; it is said to be totally integral if $L \cdot L \subseteq \mathfrak{o}$. Note that $N(L) \subseteq L \cdot L \subseteq \frac{1}{2} N(L)$.

By $a \circ L$ we will mean the lattice L on the same vector space V, but provided with the new metric $x \circ y = a(x \cdot y)$. This is not to be confused with the lattice aL which consists of the set of vectors az in the same space V provided with the same metric $x \cdot y$, where $z \in L$. But we have $a^2 \circ L \cong aL$.

The lattice J will be called a component of L if there exists a lattice K such that $L = J \oplus K$; K is then called the orthogonal complement of J in L.

A lattice L in V will be called π^i-unitary, or simply *unitary*, if

$$x \in L, x \notin \pi L \implies x \cdot L = \pi^i \mathfrak{o};$$

we call a unitary lattice L *proper* if $N(L) = L \cdot L$, otherwise *improper*. Note that if L is π^i-unitary in V, then $x \cdot L \subseteq \pi^i \mathfrak{o}$ whenever $x \in L$. And we also have

$$(3) \qquad x \in FL, x \notin L \implies |x \cdot L| > |\pi^i|;$$

for we can choose $\alpha \in \pi \mathfrak{o}$ such that $\alpha x \in L$, $\alpha x \notin \pi L$, and so $|x \cdot L| > |\pi^i|$. It is easy to see that any component of a π^i-unitary lattice is itself π^i-unitary; and conversely, the orthogonal sum of two π^i-unitary lattices is π^i-unitary. It is obvious that if L is π^i-unitary, then $\pi^\lambda \circ L$ is $\pi^{i+\lambda}$-unitary. We shall see later that L is π^0-unitary if and only if it is totally integral with determinant a unit.

1. The simplest invariant substructures.

Let us consider a lattice L on V.

DEFINITION 1. *If i is a positive or negative integer, we call*

$$L_{(i)} = \{x \mid x \in L \text{ and } x \cdot L \subseteq \pi^i \mathfrak{o}\}$$

the i-th invariant substructure of L.

The $\mathfrak{o}$-module $L_{(i)}$ defined in this way is a lattice on V; it is n-dimensional since

$$\pi^i (L \cdot L)^{-1} L \subseteq L_{(i)} \subseteq L.$$

By way of example we see that L is totally integral if and only if $L = L_{(0)}$; and $(\pi^{\lambda} \circ L)_{(\lambda+i)} = \pi^{\lambda} \circ L_{(i)}$. Note that

$$(4) \qquad \pi^{j-i} L_{(i)} \subseteq L_{(j)} \subseteq L_{(i)} \qquad \text{if } i \leqq j.$$

PROPOSITION 1. *If J is a π^{i}-unitary sublattice of L, then J is a component of L if and only if $J \subseteq L_{(i)}$.*

Proof. We need only prove the sufficiency. We can take $i = 0$. The vector space FJ being non-degenerate, we have $V = FJ \oplus (FJ)^{\perp}$ by Satz 1 of [WI]. Put $K = (FJ)^{\perp} \cap L$. Then K is a lattice on $(FJ)^{\perp}$. Now any $x \in L$ can be written uniquely in the form $w + z$ with $w \in FJ$ and $z \in (FJ)^{\perp}$. If $w \notin J$, then $| w \cdot J | > 1$ since J is unitary. Hence $| x \cdot J | > 1$, and this is impossible since $J \subseteq L_{(0)}$. Hence $w \in J$, and so $z \in K$. This proves the proposition.

It follows immediately from this proposition that every lattice L is an orthogonal sum of 1- or 2-dimensional unitary lattices. To see this we put $(x \cdot y)\mathfrak{o} = L \cdot L = \pi^{k}\mathfrak{o}$ where $x \in L$, $y \in L$; then if $x^{2}\mathfrak{o} = \pi^{k}\mathfrak{o}$, $\mathfrak{o}x$ will be a π^{k}-unitary lattice in $L = L_{(k)}$, hence a component of L; otherwise $| x^{2} | < | \pi^{k} |$, say; then $\mathfrak{o}x + \mathfrak{o}y$ is π^{k}-unitary, hence a component of L. Induction completes the proof. By regrouping these components we get the result of Section 2 [OI], that every lattice L has a *canonical decomposition* $L = L_{1} \oplus \cdots \oplus L_{t}$, where the components L_{λ} are $\pi^{s(\lambda)}$-unitary with $s(1) < s(2) < \cdots < s(t)$.

Now let L be a totally integral lattice with determinant a unit. If we express L as a canonical decomposition $L = \sum L_{\lambda}$ we must have $s(1) \geqq 0$; since $d(L)$ is a unit, it follows that $s(1) = 0$ and $t = 1$. Conversely, let L be a π^{0}-unitary lattice; then L is certainly totally integral. Express L as an orthogonal sum of 1- or 2-dimensional lattices. We can suppose that all 2-dimensional components have norms in $\pi\mathfrak{o}$. Hence $d(L)$ is a unit. We have therefore proved that *L is a π^{0}-unitary lattice if and only if L is totally integral with determinant a unit.*

Consider the canonical decomposition $L = \sum L_{\lambda}$. We contend that

$$(5) \qquad L_{(i)} = \sum_{1}^{j} \pi^{i-s(\lambda)} L_{\lambda} \oplus \sum_{j+1}^{t} L_{\lambda},$$

where j is such that $s(j) \leqq i < s(j+1)$. To prove this we write K for the right hand side of (5). If $\lambda \geqq j+1$, then $L_{\lambda} \cdot L = \pi^{s(\lambda)}\mathfrak{o} \subseteq \pi^{s(j+1)}\mathfrak{o} \subseteq \pi^{i}\mathfrak{o}$, and so $L_{\lambda} \subseteq L_{(i)}$; if $\lambda \leqq j$, then $(\pi^{i-s(\lambda)} L_{\lambda}) \cdot L_{\lambda} = \pi^{i}\mathfrak{o}$ and so $\pi^{i-s(\lambda)} L_{\lambda} \subseteq L_{(i)}$. Hence $K \subseteq L_{(i)}$. On the other hand, if $x \in L_{(i)}$ we have $x = \sum x_{\lambda}$ with $x_{\lambda} \in L_{\lambda}$;

then $x_\lambda \cdot L_\lambda \subseteq \pi^i o$ and so $x_\lambda \in \pi^{i-s(\lambda)} L_\lambda$ when $\lambda \leqq j$. Hence $L_{(i)} \subseteq K$. This proves the contention. In particular,

$$L_{(s(i))} = \sum_{1}^{i} \pi^{s(i)-s(\lambda)} L_\lambda \oplus \sum_{i+1}^{t} L_\lambda. \tag{6}$$

We see that $\pi^{s(i)-s(\lambda)} L_\lambda$ is now a $\pi^{2s(i)-s(\lambda)}$-unitary lattice; thus L_i is the first component in the canonical decomposition for $L_{(s(i))}$ that is induced by (6).

Consider another canonical decomposition $L = \sum K_\lambda$ for L in which K_λ is $\pi^{\sigma(\lambda)}$-unitary for $1 \leqq \lambda \leqq \tau$. Suppose no K_λ is $\pi^{s(i)}$-unitary for a certain fixed i $(1 \leqq i \leqq t)$. Then $L_{(s(i))}$ has the form (6); but we also have

$$L_{(s(i))} = \sum_{1}^{j} \pi^{s(i)-\sigma(\lambda)} K_\lambda \oplus \sum_{j+1}^{\tau} K_\lambda$$

where $\sigma(j) < s(i) < \sigma(j+1)$. Using the fact that $L_{(s(i))} \cdot L_{(s(i))} = \pi^{s(i)} o$, we see that this equation is impossible. Hence $t = \tau$ and $s(\lambda) = \sigma(\lambda)$ for $1 \leqq \lambda \leqq t$. We now show that $\dim L_i = \dim K_i$ and $N(L_i) \equiv N(K_i) \bmod \pi^{s(i)+1}$. By considering $L_{(s(i))}$ instead of L, we see that it suffices to consider the case $i = 1$, $s(1) = 0$. Since the first components are the only ones that can possibly represent units, it follow that $N(L_1) \equiv N(K_1) \bmod \pi$; in other words, L_1 is proper if and only if K_1 is proper. Now let M_1 denote the matrix of L in any basis corresponding to $\sum L_\lambda$; let M_2 correspond to the decomposition $\sum K_\lambda$. If $\bar{M}_1$ denotes the matrix M_1 when read in the residue class field, we see that there exists a non-singular matrix $\bar{X}$ such that $\bar{X}^T \bar{M}_1 \bar{X} = \bar{M}_2$, since M_1 and M_2 are integrally equivalent. But rank $\bar{M}_1 = \dim L_1$. And similarly with M_2. Hence $\dim L_1 = \dim K_1$. We therefore see that for two decompositions $\sum L_\lambda$ and $\sum K_\lambda$ we have

$$s(\lambda) = \sigma(\lambda), \quad \dim L_\lambda = \dim K_\lambda, \quad L_\lambda \text{ proper} \Leftrightarrow K_\lambda \text{ proper},$$

for $1 \leqq \lambda \leqq t = \tau$. Thus we have proved Theorem 3.1 of [OI] without computation. Any two lattices $L = \sum L_\lambda$ and $K = \sum K_\lambda$ which satisfy these equations are said to be *of the same type*.

DEFINITION 2. *Put* $\pi^{u(i)} o = N(L_{(s(i))})$ *for* $1 \leqq \lambda \leqq t$.

Immediately we see that

$$|2\pi^{s(i)}| \leqq |\pi^{u(i)}| \leqq |\pi^{s(i)}|; \tag{7}$$

while if $\sum L_\lambda$ is a canonical decomposition of L we must have

$$N(L_i) \subseteq \pi^{u(i)} o. \tag{8}$$

If $\dim L_i$ is odd, L_i has at least one 1-dimensional component and so L_i is proper. In this case $N(L_i) = \pi^{s(i)}\mathfrak{o} = \pi^{u(i)}\mathfrak{o}$.

DEFINITION 3. *If* $L = \sum L_\lambda$ *is a canonical decomposition of* L, *put*

$$\mathcal{R} L = \pi^{-s(t)} L_{(s(t))} = \pi^{-s(t)} L_t \oplus \cdots \oplus \pi^{-s(1)} L_1 ;$$

and when $s(i+1) = 0$, *put*

$$\mathcal{P} L = L_{(0)} = \pi^{-s(1)} L_1 \oplus \cdots \oplus \pi^{-s(i)} L_i \oplus L_{i+1} \oplus \cdots \oplus L_t .$$

We see that the decomposition for $\mathcal{P} L$ in this definition may cease to be canonical. Note that $\mathcal{R}\mathcal{R} L = L$ and $\mathcal{P}\mathcal{P} L = \mathcal{P} L$. If $s(1) = 0$, then $\mathcal{P} L = L$; if $s(t) = 0$, then $\mathcal{P} L = \mathcal{R} L$.

We know that $N(L_i) \subseteq \pi^{u(i)}\mathfrak{o}$. Can $N(L_i) = \pi^{u(i)}\mathfrak{o}$ ever be attained by a canonical decomposition $L = \sum L_\lambda$? We shall show more than this. In fact, we shall exhibit a saturated decomposition $L = \sum J_\lambda$ for L in which $N(J_\lambda) = \pi^{u(\lambda)}\mathfrak{o}$ for all λ $(1 \leqq \lambda \leqq t)$.

DEFINITION 4. *The component* L_j *of the canonical decomposition* $L = \sum L_\lambda$ *is said to be saturated if* $u(j) = \operatorname{ord} N(L_j)$; *the decomposition* $\sum L_\lambda$ *is called saturated if all its components are saturated.*

PROPOSITION 2. *L has a saturated decomposition.*

Proof. Let $L = \sum L_\lambda$ be a canonical decomposition such that $N(L_\lambda) = \pi^{u(\lambda)}\mathfrak{o}$ for $\lambda = 1, 2, \cdots, j-1$ where $1 \leqq j \leqq t$. We must extend this property to $\lambda = j$. We can assume that $s(j) = 0$. If $N(L_j \oplus \cdots \oplus L_t) = \pi^{u(j)}\mathfrak{o}$, we can take a canonical decomposition $J_j \oplus \cdots \oplus J_t$ for $L_j \oplus \cdots \oplus L_t$ in which $N(J_j) = \pi^{u(j)}\mathfrak{o}$, and we are through. Now assume that $|N(L_j \oplus \cdots \oplus L_t)| < |\pi^{u(j)}|$. Then by (6) there exists a $k < j$ such that $N(\mathcal{R} L_k) = N(\pi^{-s(k)} L_k) = \pi^{u(j)}\mathfrak{o} = \pi^{u(k)-2s(k)}\mathfrak{o}$.

Consider $\mathcal{R} L = \cdots \oplus L_j \oplus \cdots \oplus \mathcal{R} L_k \oplus \cdots$. Then

$$L_j \oplus \mathcal{R} L_k = L_j \oplus \pi^{-s(k)} L_k = J_j \oplus J_k$$

with $N(J_j) = \pi^{u(j)}\mathfrak{o}$, since $\mathcal{R} L_k$ has norm $\pi^{u(j)}\mathfrak{o}$. We then have $L_k \oplus L_j = \mathcal{R} J_k \oplus J_j$, where J_j has the required norm, while $\mathcal{R} J_k$ continues to have norm $\pi^{u(k)}\mathfrak{o}$ since

$$|N(J_j)| = |\pi^{u(j)}| = |\pi^{u(k)-2s(k)}| < |N(L_k \oplus L_j)| = |N(\mathcal{R} J_k \oplus J_j)|.$$

Then $L = \sum_{\lambda \neq j,k} L_\lambda \oplus \mathcal{R} J_k \oplus J_j$ is a canonical decomposition which extends the required property to j. Repeating this to $\lambda = t$ proves the result.

COROLLARY 2. *L_j is a saturated component of $L = \sum L_\lambda$ if and only if $\mathfrak{R} L_j$ is a saturated component of $\mathfrak{R} L = \sum \mathfrak{R} L_\lambda$.*

Proof. Suppose that L_j is saturated, but that $\mathfrak{R} L_j$ is not. Let $L = \sum K_\lambda$ be such that $\mathfrak{R} K_j$ is saturated in $\sum \mathfrak{R} K_\lambda$. Then $|N(\mathfrak{R} K_j)| > |N(\mathfrak{R} L_j)|$, and so $|N(K_j)| > |N(L_j)|$, which is impossible. On the other hand, if $\mathfrak{R} L_j$ is saturated, then so is $\mathfrak{R}\mathfrak{R} L_j = L_j$. q. e. d.

From this follows

$$u_L(j) = 2s(j) + u_{\mathfrak{R}L}(t - j + 1). \tag{9}$$

And relation (4) implies

$$|\pi^{u(i)}| \geqq |\pi^{u(j)}|, \qquad |\pi^{u(j)-2s(j)}| \geqq |\pi^{u(i)-2s(i)}| \qquad \text{if } i \leqq j. \tag{10}$$

2. Canonical bases. We have seen that any lattice L can be decomposed into an orthogonal sum of 1- and 2-dimensional unitary lattices. By choosing a basis for each of these components we can induce a minimal basis on L. Call this basis $\langle x \rangle$ and put $t(\lambda) = \operatorname{ord} x_\lambda \cdot L$; suppose that $t(1) \leqq t(2) \leqq \cdots \leqq t(n)$. Then the basis obtained in this way is said to be *semi-canonical.* If we group vectors, we get a corresponding canonical decomposition for L, and so the quantities $t(\lambda)$ are independent of $\langle x \rangle$. Thus x_λ will either be orthogonal to all the other basis vectors, and $\mathfrak{o} x_\lambda$ will then be $\pi^{t(\lambda)}$-unitary; or there is precisely one basis vector $x_{\lambda-1}$, say, which is not orthogonal to x_λ, and then $t(\lambda) = t(\lambda - 1)$ with $\mathfrak{o} x_{\lambda-1} + \mathfrak{o} x_\lambda$ unitary.

Consider the semi-canonical basis $\langle x \rangle$ for L. Generalizing a certain change of basis used in [OI], [OII], we introduce a transformation which will be denoted by the symbol $\operatorname{op}(x_i \to x_i + \alpha x_j)$. Let x_{i-1} denote that vector (if any) which is not orthogonal to x_i; let x_{j+1} denote that vector (if any) which is not orthogonal to x_j. We assume that

$$\alpha \in \mathfrak{o}, \qquad t(j) \geqq t(i), \qquad i \neq j, \qquad x_i \cdot x_j = 0.$$

Suppose that we write $\operatorname{op} x_i = x_i + \alpha x_j$. We make the further assumption that $\mathfrak{o}(\operatorname{op} x_i)$, respectively $(\mathfrak{o} x_{i-1} + \mathfrak{o}(\operatorname{op} x_i))$, are still $\pi^{t(i)}$-unitary; in other words, we assume that

$$|(\operatorname{op} x_i)^2| = |\pi^{t(i)}|, \qquad |(\operatorname{op} x_i)^2 (x_{i-1})^2 - (x_{i-1} \cdot x_i)^2| = |\pi^{2t(i)}|,$$

respectively. The transformation then consists in replacing x_i by the basis vector $\operatorname{op} x_i = x_i + \alpha x_j$ and leaving all other basis elements fixed, with the exception of x_j and (possibly) x_{j+1} which are defined in the following way:

$$(11) \quad \operatorname{op} x_j = x_j + A(\operatorname{op} x_i) + Bx_{i-1}, \quad \operatorname{op} x_{j+1} = x_{j+1} + A'(\operatorname{op} x_i) + B'x_{i-1},$$

where, if $x_i \cdot x_{i-1} = 0$,

$$(11\text{a}) \quad A = -\alpha x_j^2/(\operatorname{op} x_i)^2, \quad A' = -\alpha(x_j \cdot x_{j+1})/(\operatorname{op} x_i)^2, \quad B = 0 = B',$$

and, if $x_i \cdot x_{i-1} \neq 0$,

$$(11\text{b}) \quad \begin{aligned} A &= -\alpha x_j^2 x_{i-1}^2/D, & A' &= -\alpha(x_j \cdot x_{j+1}) x_{i-1}^2/D, \\ B &= \alpha x_j^2 (x_i \cdot x_{i-1})/D, & B' &= \alpha(x_j \cdot x_{j+1})(x_i \cdot x_{i-1})/D \end{aligned}$$

where $D = (\operatorname{op} x_i)^2 (x_{i-1})^2 - (x_i \cdot x_{i-1})^2$. By inspection, A, B, A', B', are all integers. Hence in (11b) we have

$$(\mathfrak{o}x_{i-1} + \mathfrak{o}x_i) \oplus \mathfrak{o}x_j = (\mathfrak{o}x_{i-1} + \mathfrak{o}(\operatorname{op} x_i)) \oplus (\mathfrak{o}(\operatorname{op} x_j))$$

or

$$(\mathfrak{o}x_{i-1} + \mathfrak{o}x_i) \oplus (\mathfrak{o}x_j + \mathfrak{o}x_{j+1}) = (\mathfrak{o}x_{i-1} + \mathfrak{o}(\operatorname{op} x_i)) \oplus (\mathfrak{o}(\operatorname{op} x_j) + \mathfrak{o}(\operatorname{op} x_{j+1}));$$

and similar equations hold for (11a). We see that the resulting basis for L is still semi-canonical. This is the transformation indicated by $\operatorname{op}(x_i \to x_i + \alpha x_j)$. We call the new basis $\langle \operatorname{op} x \rangle$.

As a simple example on the use of these transformations we see that any semi-canonical basis for a unitary lattice can be refined to a *canonical* basis ([OI], Definition 2.1). This can be done with each component of a general lattice; every lattice must therefore have a canonical basis ([OI], Theorem 2.4).

Using these transformations it is possible to find a special kind of basis for a π^0-unitary lattice. Let $\pi^u \mathfrak{o} = N(L)$, and put $\pi^v \mathfrak{o} = \sum x^2 \mathfrak{o} + 2\mathfrak{o}$ with $x \in L$, $u + \operatorname{ord} x^2$ odd. Then there is a decomposition

$$(12) \qquad L = L_1 \oplus L_2 \oplus \sum H_\lambda$$

and a unit ϵ, such that

$$(13) \quad L_1 \cong \epsilon \text{ if } \dim L \text{ is odd, } L_1 \cong \begin{pmatrix} \epsilon\pi^u & 1 \\ 1 & \{\pi^v\} \end{pmatrix} \text{ if } \dim L \text{ is even,}$$

$$(14) \qquad L_2 \cong \begin{pmatrix} \pi^v & 1 \\ 1 & \{4\pi^{-v}\} \end{pmatrix}, \qquad H_\lambda \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

We have discussed these decompositions in Sections 14, 17, 18 of [OI] and proofs are omitted here.

instead of for the given I and J. In virtue of Proposition 1, we can write $I \oplus L = I \oplus L_1 \oplus L_2$ with $L_1 \cong \epsilon$. Now $I \oplus L_1 = H \oplus L_1' \cong H \oplus L_1$ where H is a unit hyperbolic plane. And similarly with K. Hence $H \oplus L \cong I \oplus L \cong J \oplus K \cong H' \oplus K$. Hence $L \cong K$ by Proposition 3. q. e. d.

4. Supersaturated decompositions. It is our intention here to show that the numbers represented by $L_{(s(j))}$ can be described in a simple way in terms of the quantities a_j and $v(j)$ defined below. We shall then show that any big lattice has a canonical decomposition in which the j-th component represents all numbers represented by the $s(j)$-th invariant substructure.

DEFINITION 5. *For each* j $(1 \leqq j \leqq t)$, *put* $\pi^{v(j)}\mathfrak{o} = \sum \mathfrak{o}x^2 + 2\pi^{s(j)}\mathfrak{o}$ *where* x *runs through all vectors in* $L_{(s(j))}$ *for which* ord x^2 *and* $u(j)$ *have opposite parity.*

We immediately see that

$$u(j) \leqq v(j) \leqq e + s(j), \tag{15}$$

$$u(j) = v(j) \Leftrightarrow u(j) = e + s(j), \tag{16}$$

$$v(j) < e + s(j) \Longrightarrow u(j) + v(j) \text{ odd.} \tag{17}$$

PROPOSITION 4. *There exists an* a_j *of ordinal* $u(j)$ *such that every number represented by* $L_{(s(j))}$ *is of the form* $a_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o}$.

Proof. Take $x_0 \in L_{(s(j))}$ of norm $\pi^{u(j)}\mathfrak{o}$ and define $a_j = x_0^2$. Suppose that $x \in L_{(s(j))}$ cannot be expressed in the required form. Then $|\pi^{v(j)}| < |x^2| \leqq |a_j|$ and so $u(j)$ and ord x^2 must have the same parity. In virtue of the perfectness of the residue class field we can take $x^2 = \beta^2 a_j(1 + [\pi^\gamma])$ where $\beta \in \mathfrak{o}$ and $|\pi^\gamma| < 1$. Suppose that β and γ have been chosen so that γ is maximal for the given x. Then $|\pi^\gamma| > |2|$ since x^2 does not have the desired form. Hence γ is odd by (1). But $|(x + \beta x_0)^2| = |\beta^2 a_j \pi^\gamma| > |\pi^{v(j)}|$, and this is impossible by definition of $v(j)$. q. e. d.

From now on we shall understand by $a_j = a_j(L)$ a fixed element of F which describes $L_{(s(j))}$ according to Proposition 4. If $\bar{a}_j$ is used instead of a_j, then $a_j \cong \bar{a}_j \bmod \pi^{v(j)}$. Note that the elements of the form $a_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o}$ form an additive group in F. This follows from the relation

$$a_j\alpha_1^2 - a_j\alpha_2^2 \equiv a_j(\alpha_1 - \alpha_2)^2 \bmod \pi^{v(j)}.$$

We see that $\bar{a}_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o} = a_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o}$ if $\bar{a}_j \cong a_j \bmod \pi^{v(j)}$. In particular, such an $\bar{a}_j$ can be used instead of a_j in Proposition 4. Consider the quantities

$s(j)$, $u(j)$, $v(j)$, a_j for L; if $S(j)$, $U(j)$, $V(j)$, A_j are the same quantities computed for $(\pi^k \circ L)$, then $S(j) = s(j) + k$ and so $(\pi^k \circ L)_{(S(j))} = \pi^k \circ L_{(s(j))}$; hence

$$U(j) = u(j) + k, \qquad V(j) = v(j) + k, \qquad A_j \cong a_j \pi^k \bmod \pi^{V(j)}.$$

DEFINITION 6. *We say that the component L_j of the canonical decomposition $\sum L_\lambda$ is supersaturated if L_j represents all numbers of the form $a_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o}$. The decomposition $\sum L_\lambda$ is called supersaturated if all its components are supersaturated.*

It follows from (6) that if a lattice has a supersaturated component L_j, then $L_{(s(j))}$ represents all numbers in the additive group $a_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o}$. In particular, L_j and $L_{(s(j))}$ then represent the same numbers. Clearly a supersaturated component must be saturated. We would like to proceed as we did with the saturated decompositions and we ask whether every lattice must have at least one supersaturated decomposition. In general the answer must be no: for what can be done with a 1-dimensional component? But the result is true for big lattices and we shall establish it after proving the next two propositions.

PROPOSITION 5. *If L is π^0-unitary and $\dim L \geqq 5$, then L represents every number of the form $a_1\mathfrak{o}^2 + \pi^{v(1)}\mathfrak{o}$.*

Proof. It suffices to prove the result for an a_1 that is actually represented by L. Select $x_1 \in L$ such that $x_1{}^2 = a_1$. It follows from (12) and (14) that there is a vector $x_2 \in L$ such that $x_2{}^2 = \pi^{v(1)}$. Now let α be a number of the form $a_1\mathfrak{o}^2 + \pi^{v(1)}\mathfrak{o}$. We must prove that L represents α. Suppose that L represents $\alpha + \epsilon\pi^\gamma$ where ϵ is a unit, but that L does not represent $\alpha + \{\pi^{\gamma+1}\}$. Then $|\pi^\gamma| \leqq |\pi^{v(1)}|$.

(i) Let $|\pi^\gamma| > |2|$. Then $u(1)$ and $v(1)$ have opposite parity. Suppose that $z^2 = \alpha + \epsilon\pi^\gamma$. If γ and $v(1)$ are of the same parity, then by the perfectness of the residue class field there is a $\beta \in \mathfrak{o}$ such that $(z + \beta x_2)^2 \equiv \alpha \bmod \pi^{\gamma+1}$, and this is impossible by definition of γ. Hence $\gamma + u(1)$ is even. Using x_1 instead of x_2 shows that this is impossible. Hence (ii) let $|\pi^\gamma| \leqq |2|$. Then we write $L = H \oplus K$ where H is a hyperbolic plane, and we see that K must represent $\alpha + \epsilon\pi^\gamma \bmod 2$. Select $w \in K$ such that $w^2 = \alpha + 2\delta\pi^\Gamma$, and then $y \in H$ such that $y^2 = -2\delta\pi^\Gamma$. We see that $w + y$ is the vector required. This proves the proposition.

PROPOSITION 6. *L is a big π^0-unitary lattice and α is represented by L. Then there is a decomposition $L = L_1 \oplus L_2$ where L_2 represents the same numbers as L, and $L_1 \cong \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}$.*

Proof. Write $L = H \oplus K$ where H is a hyperbolic plane. Then $u_K(1) = u_L(1)$ and $v_K(1) = v_L(1)$, so that L and K represent the same numbers by Propositions 4 and 5. It is easily seen that corresponding to this decomposition we can write

$$H \oplus K \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix} \oplus \cdots.$$

Call the corresponding basis $x_1, x_2, x_3, \cdots$ and apply $\operatorname{op}(x_1 \to x_1 + x_3)$. Using equations (11) and (11b) this gives $H \oplus K = H' \oplus K'$ with $H' \cong \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}$, and it follows by inspection that $K \cong K'$. Hence $L = H' \oplus K'$ is the required decomposition. This proves the proposition.

PROPOSITION 7. *If L is big, it has a supersaturated decomposition.*

Proof. Suppose that we have found a saturated decomposition $L = \sum K_\lambda$ such that the components K_λ are supersaturated for $\lambda = 1, 2, \cdots, j-1$ where $1 \leqq j \leqq t$. We must extend this property to $\lambda = j$. We can take $s(j) = 0$ and $|\pi^{v(j)}| > |2|$. Then for each λ $(1 \leqq \lambda \leqq t)$ there is an α_λ represented by K_λ such that

$$|\pi^{-2s(1)}\alpha_1 + \cdots + \pi^{-2s(j-1)}\alpha_{j-1} + \alpha_j + \cdots + \alpha_t| = |\pi^{v(j)}|,$$

since $L_{(s(j))}$ represents $[\pi^{v(j)}]$. By Proposition 6, write $K_\lambda = (\mathfrak{o}x_\lambda + \mathfrak{o}y_\lambda) \oplus K_\lambda{}^*$ where $K_\lambda{}^*$ represents the same numbers as K_λ, and $x_\lambda{}^2 = \alpha_\lambda$, $y_\lambda{}^2 = 0$. Then

$$x = \pi^{-s(1)}x_1 + \cdots + \pi^{-s(j-1)}x_{j-1} + x_j + \cdots + x_t$$

is in $L_{(s(j))}$ and $(\mathfrak{o}x + \mathfrak{o}y_j)$ is unitary. Hence $(\mathfrak{o}x + \mathfrak{o}y_j)$ is a component for the lattice $\sum(\mathfrak{o}x_\lambda + \mathfrak{o}y_\lambda)$. This yields a new saturated decomposition $L = \sum J_\lambda$ in which the J_λ are still supersaturated when $1 \leqq \lambda \leqq j-1$, while J_j now represents a number of ordinal $v(j)$ and is therefore supersaturated in virtue of Proposition 5. Thus we have extended our result to $\lambda = j$. Proceeding to $\lambda = t$ proves the result.

COROLLARY 7. *L_j is a supersaturated component of the big lattice $L = \sum L_\lambda$ if and only if $\mathfrak{R}L_j$ is a supersaturated component of $\mathfrak{R}L = \sum \mathfrak{R}L_\lambda$.*

Proof. Similar to Corollary 2.

We remark that if we enlarge a given lattice by adjoining $\pi^{s(i)}$-hyperbolic planes, then the enlarged lattice has the same a's and v's as the original one. We can easily see that

$$v_L(j) = 2s(j) + v_{\mathfrak{R}L}(t - j + 1) \tag{18}$$

holds for a big lattice. By the last remark it must therefore be true in general.

Let L^* denote a big lattice obtained by adjoining $\pi^{s(i)}$-hyperbolic planes to L. Associated with $L_{(s(j))}$ is the group $a_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o}$, and the same group is associated with $L_{(s(j))}{}^*$; we know that the elements of this group are precisely the numbers represented by $L_{(s(j))}{}^*$. By considering the relation

$$L_{(s(i))}{}^* \supseteq L_{(s(j))}{}^* \supseteq \pi^{s(j)-s(i)} L_{(s(i))}{}^*$$

we see that

$$a_i\mathfrak{o}^2 + \pi^{v(i)}\mathfrak{o} \supseteq a_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o},\quad \pi^{-2s(i)}(a_i\mathfrak{o}^2 + \pi^{v(i)}\mathfrak{o}) \subseteq \pi^{-2s(j)}(a_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o}) \tag{19}$$

holds for L if $i \leqq j$.

5. The ideal $\mathfrak{f}_j$. We now introduce $\mathfrak{f}_j$ for values of j in $1 \leqq j \leqq t - 1$. This is an ideal defined in terms of the u's and v's in the following way:

(i) *if* $u(j)$ *and* $u(j+1)$ *have opposite parity, put* $\pi^{2s(j)}\mathfrak{f}_j = \pi^{u(j)+u(j+1)}\mathfrak{o}$;

(ii) *if* $u(j)$ *and* $u(j+1)$ *have the same parity, let* $\pi^{2s(j)}\mathfrak{f}_j$ *be the ideal generated by* $\pi^{u(j)+u(j+1)}\mathfrak{g}(a_ja_{j+1})$, $\pi^{u(j)+v(j+1)}$, $\pi^{u(j+1)+v(j)}$, $2\pi^{(u(j)+u(j+1))/2+s(j)}$.

We note that $\mathfrak{f}_j$ has the same value if we replace a_j, a_{j+1} by $a_j + \{\pi^{v(j)}\}$, $a_{j+1} + \{\pi^{v(j+1)}\}$, respectively. In other words, the representative of $a_j \bmod \pi^{v(j)}$ is immaterial. It is easily seen from (9) and (18) that $\mathfrak{f}_j(L) = \mathfrak{f}_{t-j}(\mathfrak{R}L)$; and $\mathfrak{f}_j(\alpha \circ L) = \mathfrak{f}_j(L)$. Since the u's, v's and a's are unaltered by the adjunction of $\pi^{s(i)}$-hyperbolic planes which leave the type unaltered, it follows that such an adjunction cannot alter the $\mathfrak{f}$'s. By considering a supersaturated decomposition of a big lattice, we see that for any L, $|\pi^{-u(j)}\mathfrak{f}_j| \leqq |\pi^{v(j)}|$ when $s(j) = 0$. Thus $\mathfrak{f}_j$ is always contained in $\pi\mathfrak{o}$. Note that if $L = \sum L_\lambda$ is supersaturated, then

$$\mathfrak{f}_j(L) = \mathfrak{f}_1(L_j \oplus L_{j+1}). \tag{20}$$

Let $\langle x \rangle$ denote a semi-canonical basis for L and put $t(\lambda) = \operatorname{ord}(x_\lambda \cdot L)$. Then we shall have occasion to use the relation

$$x_\lambda{}^2 x_\mu{}^2 \mathfrak{g}(x_\lambda{}^2 x_\mu{}^2) \subseteq \pi^{2t(\lambda)}\mathfrak{f}_j \tag{21}$$

where $x_\lambda \in L_1 \oplus \cdots \oplus L_j$, $x_\mu \in L_{j+1} \oplus \cdots \oplus L_t$. To prove the validity of this relation, we take $s(j) = 0$ and note that $\pi^{-t(\lambda)} x_\lambda \in L_{(s(j))}$, hence $\pi^{-2t(\lambda)} x_\lambda^2 = \alpha^2 a_j + \{\pi^{v(j)}\}$ with α an integer; similarly $x_\mu^2 = \beta^2 a_{j+1} + \{\pi^{v(j+1)}\}$. Hence (21) follows from the definition of $\mathfrak{f}_j$.

The u's and v's take on a simpler form when $s(j+1) = s(j) + 1$. For instance, it follows from (10) that

$$(22) \qquad |\pi^{u(j)+2}| \leqq |\pi^{u(j+1)}| \leqq |\pi^{u(j)}|.$$

So we find

$$(23) \qquad u(j+1) = u(j) \Longrightarrow \pi^{2s(j)}\mathfrak{f}_j = \pi^{u(j)+v(j)}\mathfrak{o},$$

$$(24)\ u(j+1) = u(j) + 1 \Longrightarrow \pi^{2s(j)}\mathfrak{f}_j = \pi^{2u(j)+1}\mathfrak{o},$$

$$(25)\ u(j+1) = u(j) + 2 \Longrightarrow \pi^{2s(j)}\mathfrak{f}_j = \pi^{u(j)+v(j+1)}\mathfrak{o} \text{ if } s(j+1) = s(j) + 1.$$

The result (23) follows by observing that we can take $a_j = a_{j+1}$, that $v(j+1) \geqq v(j)$, and that $|2\pi^{(u(j)+u(j+1))/2+s(j)}| \leqq |\pi^{u(j+1)+v(j)}|$. The result (24) is trivial. The result (25) follows by taking $a_{j+1} = a_j \pi^2$ and noting that $v(j) \leqq v(j+1) \leqq v(j) + 2$, $|2\pi^{(u(j)+u(j+1))/2+s(j)}| \leqq |\pi^{u(j)+v(j+1)}|$. It is clear from the proofs that (23) and (24) hold even if $s(j+1) \neq s(j) + 1$.

The next lemma will be used in proving the necessity of Theorem 2. We shall establish this lemma in full generality in Theorem 3.

LEMMA 1. *Let* $L = \sum K_\lambda = \sum J_\lambda$ *be two canonical decompositions of* L *such that* $N(K_1) = \pi^{u(1)}\mathfrak{o} = N(J_1)$ *and* $s(1) = 0$, *where* $\dim K_1 = \dim J_1$ *is even and* $\geqq 4$. *Then* $K_1 \cong J_1 \pmod{\mathfrak{f}_1 \pi^{-u(1)}}$ *and* $d(K_1)/d(J_1) \cong 1 \bmod \mathfrak{f}_1$.

Proof. We put $\mathfrak{b}_1 = \pi^{-u(1)}\mathfrak{f}_1$; then we have $\mathfrak{b}_1 = \pi^{u(2)}\mathfrak{o}$ if $u(1) + u(2)$ is odd; while if $u(1)$ and $u(2)$ have the same parity we have

$$\mathfrak{b}_1 = [\pi^{u(2)}\mathfrak{g}(a_1 a_2), \pi^{v(2)}, \pi^{u(2)-u(1)+v(1)}, 2\pi^{(u(2)-u(1))/2}].$$

Using equations (12)-(14) we can express $K_1 = H \oplus K_1^*$, $J_1 = H' \oplus J_1^*$ where K_1^* and J_1^* are 4-dimensional while $H \cong H'$ are orthogonal sums of hyperbolic planes. Since the orthogonal complements of H and H' in L are isometric, it follows that we can assume that K_1 and J_1 are 4-dimensional. Let a_1 denote a number of ordinal $u(1)$ that is represented by K_1.

If $u(2) = u(1)$, then $\mathfrak{b}_1 = \pi^{v(1)}\mathfrak{o}$ and so (12)-(14) imply that

$$K_1 \cong \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cong J_1 \bmod \mathfrak{b}_1.$$

Hence we can assume that $u(2) > u(1)$. We do so from now on.

Write K_1 in a basis $(\mathfrak{o}y_1+\mathfrak{o}y_2)\oplus(\mathfrak{o}y_3+\mathfrak{o}y_4)$ in which

$$K_1\cong\begin{pmatrix}\epsilon\pi^{u(1)} & 1\\ 1 & \alpha\pi^{v(1)}\end{pmatrix}\oplus\begin{pmatrix}\delta\pi^{u(1)} & 1\\ 1 & \beta\pi^{v(1)}\end{pmatrix}$$

where ϵ and δ are units and where α and β are integers. Then there exist vectors x_1 and x_2 in J_1, X_1 and X_2 in $J=J_2\oplus\cdots\oplus J_t$, such that

$$y_1=x_1+X_1,\qquad y_2=x_2+X_2.$$

It is easily seen that $\mathfrak{o}x_1+\mathfrak{o}x_2$ is unitary and we write

$$L=(\mathfrak{o}x_1+\mathfrak{o}x_2)\oplus(\mathfrak{o}\bar{x}_3+\mathfrak{o}\bar{x}_4)\oplus J=(\mathfrak{o}y_1+\mathfrak{o}y_2)\oplus(\mathfrak{o}\bar{x}_3+\mathfrak{o}\bar{x}_4)\oplus J^*.$$

If K denotes the orthogonal complement of K_1 in L, we have

$$(\mathfrak{o}\bar{x}_3+\mathfrak{o}\bar{x}_4)\oplus J^*=(\mathfrak{o}y_3+\mathfrak{o}y_4)\oplus K.$$

Hence $y_3=z_3+Z_3$, $y_4=z_4+Z_4$, with z_3 and z_4 in $(\mathfrak{o}\bar{x}_3+\mathfrak{o}\bar{x}_4)$, and Z_3 and Z_4 in J^*. Again we see that $\mathfrak{o}z_3+\mathfrak{o}z_4$ is unitary and we get

$$\begin{aligned}L=(\mathfrak{o}y_1+\mathfrak{o}y_2)\oplus(\mathfrak{o}\bar{x}_3+\mathfrak{o}\bar{x}_4)\oplus J^*&=(\mathfrak{o}y_1+\mathfrak{o}y_2)\oplus(\mathfrak{o}z_3+\mathfrak{o}z_4)\oplus J^*\\ &=(\mathfrak{o}y_1+\mathfrak{o}y_2)\oplus(\mathfrak{o}y_3+\mathfrak{o}y_4)\oplus K.\end{aligned}$$

Now $(\mathfrak{o}x_1+\mathfrak{o}x_2)$ and $(\mathfrak{o}z_3+\mathfrak{o}z_4)$ both represent $[\pi^{u(1)}]$; so it suffices for us to prove that $(\mathfrak{o}x_1+\mathfrak{o}x_2)\cong(\mathfrak{o}y_1+\mathfrak{o}y_2)\bmod\mathfrak{b}_1$ and that $(\mathfrak{o}z_3+\mathfrak{o}z_4)\cong(\mathfrak{o}y_3+\mathfrak{o}y_4)\bmod\mathfrak{b}_1$. On grounds of symmetry, this reduces to the single problem of proving $(\mathfrak{o}x_1+\mathfrak{o}x_2)\cong(\mathfrak{o}y_1+\mathfrak{o}y_2)\bmod\mathfrak{b}_1$.

If $u(2)$ and $u(1)$ are of opposite parity, we have $x_1{}^2\equiv y_1{}^2\bmod\mathfrak{b}_1$, $x_2{}^2\equiv y_2{}^2\bmod\mathfrak{b}_1$, $x_1\cdot x_2\equiv y_1\cdot y_2\bmod\pi^{s(2)}$, and the result follows if we observe that $x_2{}^2(1+\{\pi^{s(2)}\})^2\equiv x_2{}^2\bmod\mathfrak{b}_1$.

We now assume that $u(1)<u(2)$ have the same parity. In this case $X_1{}^2=a^2a_2+\{\pi^{v(2)}\}\equiv a^2a_2\bmod\mathfrak{b}_1$; while $\epsilon\pi^{u(1)}\cong a_1\bmod\pi^{v(1)}$ implies that $\epsilon\pi^{u(2)}\cong a_2\bmod\mathfrak{b}_1$. Similarly with X_2. Hence we may take

$$X_1{}^2\equiv a^2\epsilon\pi^{u(2)}\bmod\mathfrak{b}_1,\qquad X_2{}^2\equiv b^2\epsilon\pi^{u(2)}\bmod\mathfrak{b}_1,$$

where a and b are integers. We therefore have

$$x_1{}^2\equiv\epsilon\pi^{u(1)}(1+a\pi^{\frac{1}{2}(u(2)-u(1))})^2\bmod\mathfrak{b}_1.$$

Replace x_1 and x_2 by

$$(1+a\pi^{\frac{1}{2}(u(2)-u(1))})^{-1}x_1\quad\text{and}\quad(1+a\pi^{\frac{1}{2}(u(2)-u(1))})(x_1\cdot x_2)^{-1}x_2$$

respectively. An easy computation shows that this second vector has norm

$\alpha\pi^{v(1)} - B^2\epsilon\pi^{u(2)} \bmod \mathfrak{b}_1$; so we have $(\mathfrak{o}x_1 + \mathfrak{o}x_2) \cong (\mathfrak{o}\omega_1 + \mathfrak{o}\omega_2) \bmod \mathfrak{b}_1$ where $\mathfrak{o}\omega_1 + \mathfrak{o}\omega_2$ has the matrix

$$\begin{pmatrix} \epsilon\pi^{u(1)} & 1 \\ 1 & \alpha\pi^{v(1)} - B^2\epsilon\pi^{u(2)} \end{pmatrix}, \qquad B \in \mathfrak{o}.$$

Now replace ω_2 by $(\omega_2 + B\pi^{\frac{1}{2}(u(2)-u(1))}\omega_1)\ (1 + \epsilon B\pi^{\frac{1}{2}(u(2)+u(1))})^{-1}$. Doing this we see that $(\mathfrak{o}x_1 + \mathfrak{o}x_2) \cong (\mathfrak{o}\omega_1 + \mathfrak{o}\omega_2) \cong (\mathfrak{o}y_1 + \mathfrak{o}y_2) \bmod \mathfrak{b}_1$. This proves the lemma.

PROPOSITION 8. *Let* $L = \sum I_\lambda$ *and* $L = \sum M_\lambda$ *be two canonical decompositions of* L. *If* j *is fixed* $(1 \leqq j \leqq t)$, *we can pass from* $\sum I_\lambda$ *to* $\sum M_\lambda$ *through a chain of canonical decompositions*

$$\sum I_\lambda \rightarrow \cdots \rightarrow \sum J_\lambda \rightarrow \sum K_\lambda \rightarrow \cdots \rightarrow \sum M_\lambda \tag{26}$$

such that under each transformation either (i) $\sum_1^j J_\lambda = \sum_1^j K_\lambda$ *or* (ii) $J_\lambda = K_\lambda\ (1 \leqq \lambda \leqq j-1)$.

Proof. We proceed by induction to $d = \dim(\sum_1^j I_\lambda)$. If $j = 1$ we are through. So assume that $j > 1$. We can take $s(1) = 0$. Let $\langle y \rangle$ denote a canonical basis corresponding to $\sum M_\lambda$.

Case 1. I_1 proper. Then we can write $y_1 = x_1 + X$ where $x_1 \in \sum_1^j I_\lambda$, $X \in \sum_{j+1}^t I_\lambda$. Since x_1^2 and y_1^2 are units, we can write $\sum_1^j I_\lambda$ in a canonical basis $\langle x \rangle$ having x_1 as its first element; this is the first transformation of the chain we are constructing and it satisfies the first condition of the proposition.

Apply $\operatorname{op}(x_1 \rightarrow x_1 + x_d)$ and put $X_1 = \operatorname{op} x_1$, $X_d = \operatorname{op} x_d$, $X_{d-1} = \operatorname{op} x_{d-1}$. Using (11) and (11a) it can be verified that $y_1 = \epsilon X_1 + \delta X_d + X$, where ϵ and δ are units. Put $X_d^* = X_d + \delta^{-1}X$ and express L in the semi-canonical basis

$$L = \mathfrak{o}X_1 \oplus (\mathfrak{o}x_2 + \cdots + \mathfrak{o}X_{d-1} + \mathfrak{o}X_d^*) \oplus (\mathfrak{o}z_{d+1} + \cdots + \mathfrak{o}z_n).$$

Apply $\operatorname{op}(X_1 \rightarrow X_1 + \epsilon^{-1}\delta X_d^*)$ and call the resulting basis $\langle z \rangle$. Then all the requirements of the proposition are satisfied by our chain of transformations. On the other hand $\epsilon z_1 = y_1$; we can apply the induction to the orthogonal complement of $\mathfrak{o}y_1$ to extend the chain from $\langle z \rangle$ to $\langle y \rangle$.

Case 2. I_1 improper. We can write $y_1 = x_1 + X$ with $x_1 \in \sum_1^j I_\lambda$, $X \in \sum_{j+1}^t I_\lambda$; since $y_1 \cdot y_2 = 1$, there must be a vector $x_2 \in \sum_1^j I_\lambda$ for which

$x_1 \cdot x_2 = 1$. Since $\mathfrak{o}x_1 + \mathfrak{o}x_2$ is unitary, we can suppose that x_1, x_2 is extended to a canonical basis for $\sum_1^t I_\lambda$. Apply $\operatorname{op}(x_1 \to x_1 + x_d)$ and put $X_1 = \operatorname{op} x_1$, $X_d = \operatorname{op} x_d$, $X_{d-1} = \operatorname{op} x_{d-1}$. Using (11) and (11b) it can be verified that $y_1 = \epsilon X_1 + \alpha x_2 + \delta X_d + X$, where ϵ and δ are units, $\alpha \in \mathfrak{o}$. Put $X_d{}^* = X_d + \delta^{-1} X$ and express L in the semi-canonical basis

$$L = (\mathfrak{o}(\epsilon X_1 + \alpha x_2) + \mathfrak{o}x_2) \oplus (\mathfrak{o}x_3 + \cdots + \mathfrak{o}X_{d-1} + \mathfrak{o}X_d{}^*) \oplus (\mathfrak{o}z_{d+1} + \cdots + \mathfrak{o}z_n).$$

Now apply $\operatorname{op}(\epsilon X_1 + \alpha x_2 \to \epsilon X_1 + \alpha x_2 + \delta X_d{}^*)$ and call the resulting basis $\langle z \rangle$. Note that all these transformations are admissible in the sense that they satisfy the requirements of the proposition.

We now have $y_1 = z_1$, $y_2 = a_{12}z_1 + \cdots + a_{n2}z_n$; hence

$$y_1 \cdot (a_{12}z_1 + \cdots + a_{d2}z_d) = 1.$$

Replacing z_2 by $a_{12}z_1 + \cdots + a_{d2}z_d$, we see that we can assume that $y_2 = z_2 + Z$ with $Z \in \sum_{d+1}^n \mathfrak{o}z_\lambda$. We now proceed exactly as we did with y_1, and using admissible transformations only we arrive at a basis $\sum \mathfrak{o}z_\lambda'$ in which $(\mathfrak{o}y_1 + \mathfrak{o}y_2) = (\mathfrak{o}z_1' + \mathfrak{o}z_2')$. Then $\sum_3^n \mathfrak{o}z_\lambda' = \sum_3^n \mathfrak{o}y_\lambda$, and the induction completes the proof.

6. Unitary lattices modulo $\mathfrak{p}$. The Hasse symbol $S(L)$ of a given lattice L will play an important part in the rest of the paper. In the notation of Witt [WI], $S(L)$ is the product of quaternion algebras $\prod_{\lambda \leqq \mu} (a_\lambda, a_\mu)$ where $\sum a_\lambda{}^2 x_\lambda{}^2$ is any diagonal form associated with the metric in FL. When manipulating with these symbols we will use without further reference the rules of operation established on pp. 37-38 of Witt's paper [WI]. These results are valid over general fields; in addition, we have seen on p. 98 of [OI] that in a local field whose residue class field is perfect and of characteristic 2, the following relations are true:

$$(1 + 4\alpha, \epsilon) = 1, \tag{27}$$

$$(1 + 4\alpha, \epsilon\pi) = 1 \iff (1 + 4\alpha)^{\frac{1}{2}} \in F, \tag{28}$$

for any unit ϵ and any $\alpha \in \mathfrak{o}$.

Now let k be a rational integer, $0 < k \leqq e$. We contend that the quadratic form

$$(1 + \{4\pi^{1-k}\})x^2 + (1 + \{\pi^k\})y^2$$

represents 1. To this end we consider the lattice

$$L \cong (1+\{4\pi^{1-k}\}) \oplus (1+\{\pi^{k}\}).$$

It suffices to prove that L represents 1. Let us write L in the basis $\mathfrak{o}x_1 \oplus \mathfrak{o}x_2$ in which $L \cong (1+[\pi^{\gamma}]) \oplus (1+\{\pi^{k}\})$ with γ maximal. Then $|\pi^{\gamma}| \leqq |4\pi^{1-k}| \leqq |2\pi|$. Suppose if possible that $\gamma < \infty$. Then by Hensel's lemma, $\gamma \leqq 2e$; on the other hand, γ must be an odd number or we could apply $\operatorname{op}(x_1 \to x_1 + \alpha x_2)$ with α chosen so as to increase γ. Then there is a unit E such that

$$x_1^2 = 1 + E\pi^{\gamma} = (1+\tfrac{1}{2}E\pi^{\gamma})^2 - (\tfrac{1}{2}E\pi^{\gamma})^2.$$

Hence we can in fact assume that $x_1^2 = 1 - (\frac{1}{2}E\pi^{\gamma})^2$. Now apply $\operatorname{op}(x_1 \to x_1 + \frac{1}{2}E\pi^{\gamma}x_2)$; we see that $(x_1 + \frac{1}{2}E\pi^{\gamma}x_2)^2 = 1 + \{\pi^{2\gamma+k-2e}\}$ where $|\pi^{2\gamma+k-2e}| < |\pi^{\gamma}|$, and we have increased γ, which is impossible. Hence L represents 1. So the given quadratic form must represent 1. By putting $m = 2e+1-k$ we see that this result remains valid if $e < k \leqq 2e$. Hence we have

$$(29) \qquad ((1+\{4\pi^{1-k}\}),\ (1+\{\pi^{k}\})) = 1 \qquad \text{if } 0 < k \leqq 2e.$$

We now prove that (A,B) can always be represented in the following way:

$$(30) \qquad (A,B) = (1+4C,\pi) \qquad \text{for some } C \in \mathfrak{o}.$$

First let A be a unit, B a prime; successive application of $\operatorname{op}(x_1 \to x_1 + \alpha x_2)$ to the lattice $L \cong Ax^2 + By^2$ shows that this form is equivalent to the form $(1+\{4\})x^2 + D\pi y^2$; therefore we have $(A,B) = (1+\{4\}, D\pi) = (1+\{4\},\pi)$ by (27). In general, we can suppose that A is either a unit or a prime; and similarly with B. If A and B are both units, then $(A,B) = (A,B\pi)(A,\pi) = (1+\{4\},\pi)$; if A and B are both primes, then

$$(A,B) = (B\pi^{-1},A)(-A\pi^{-1},\pi) = (1+\{4\},\pi). \qquad \text{q. e. d.}$$

In particular, (30) shows that the algebra classes (a,b) form a group over fields of our type. Now suppose that the Hasse symbols are not trivial over F. Then there is a unit ϵ such that $(1+4\epsilon)^{\frac{1}{2}} \notin F$; in other words, $x^2 + x - \epsilon$ is irreducible over F. Since this polynomial has distinct roots modulo π, it must be irreducible over the residue class field $\bar{F}$, by Hensel's lemma [AI]. Hence $\bar{F}$ has at least one quadratic extension. Conversely, let us assume that $\bar{F}$ has a quadratic extension and let $x^2 + \epsilon x + \delta$ be irreducible modulo π. Then $(1-4\delta\epsilon^{-2})^{\frac{1}{2}} \notin F$ and so the Hasse symbols are non-trivial over F.

THEOREM 1. *L and K are π^0-unitary lattices of the same dimension such that $v_L(1) = v = v_K(1)$ and $a_1(L) \cong a \cong a_1(K) \bmod \pi^v$ with $|a| \geqq |2|$. If $\mathfrak{p} \subseteq \pi^v\mathfrak{o}$, then $L \cong K \bmod \mathfrak{p}$ if and only if* (i) $d(L) \cong d \cong d(K) \bmod a\mathfrak{p}$, (ii) $(d(L), ad)S(L) = (d(K), ad)S(K)$ *when* $|\mathfrak{p}| < |4\pi^{-v}|$.

Proof. We write $|a| = |\pi^u|$.

Necessity. If we adjoin a hyperbolic plane to L and K, the resulting lattices are still isometric modulo $\mathfrak{p}$, and their u's and v's are the same as for L and K. It is easily seen that if (i) and (ii) are true for the enlarged lattices, then they are true for L and K. Hence we can assume that $\dim L = \dim K \geqq 3$. If L and K are proper, we can adjoin $J \cong (a)$ to L and K, and the same argument shows that we can assume that $\dim L = \dim K \geqq 4$ is an even number.

We have mentioned in (12)-(14) that a basis can be found for L in which $L = L_1 \oplus L_2 \oplus \sum H_\lambda$ where the H_λ are hyperbolic planes and

$$L_1 \cong \begin{pmatrix} b\pi^u & 1 \\ 1 & \{\pi^v\} \end{pmatrix}, \qquad L_2 \cong \begin{pmatrix} \pi^v & 1 \\ 1 & \{4\pi^{-v}\} \end{pmatrix}; \qquad |b| = 1.$$

Since $L \cong K \bmod \mathfrak{p}$ where $\mathfrak{p} \subseteq \pi^v\mathfrak{o}$, it follows from Lemma 2.2 in [OI] that we can obtain a decomposition $K_1 \oplus K_2 \oplus \sum M_\lambda$ for K in which

$$K_1 \cong L_1 \bmod \mathfrak{p}, \qquad K_2 \cong L_2 \bmod \mathfrak{p}, \qquad M_\lambda \cong H_\lambda \bmod \mathfrak{p}.$$

Calculating determinants in these bases proves that $d(L) \cong d(K) \pmod{\pi^u\mathfrak{p}}$, thereby proving the first result. We now define d as any unit satisfying the first relation. In order for (ii) to be non-vacuous, we assume that $\mathfrak{p} \subseteq (4\pi/\pi^v)\mathfrak{o}$. If $u = e$ we have $\mathfrak{p} \subseteq 2\pi\mathfrak{o}$, hence $L \cong K$ by Lemma 14.4 in [OI], and so (ii) holds. Hence we can suppose that $e > u$, $v > u$. Then it follows from the same result in [OI] that $L_2 \oplus \sum H_\lambda \cong K_2 \oplus \sum M_\lambda$.

We can write $K_1 \cong \begin{pmatrix} B\pi^u & 1 \\ 1 & \{\pi^v\} \end{pmatrix}$, where $B = b + \{4\pi/\pi^{u+v}\}$; we have $d_b \cong d_B + \{4\pi/\pi^{v-u}\}$ where $d_b = \det L_1$ and $d_B = \det K_1$. We know that $a\pi^{-u} \cong b \cong B \pmod{\pi^{v-u}}$. An easy calculation with Hasse symbols gives

$$(d(L), ad)S(L)\,(d(K), ad)S(K) = (bB, -d_b)\,(d_b d_B, -a\pi^u B d d_b d(L)).$$

Using (29) it is easily verified that this expression is equal to 1. Hence we have $(d(L), ad)S(L) = (d(K), ad)S(K)$, and this proves the result.

Sufficiency. If L and K each contain a hyperbolic plane, then it is easily seen that (i) and (ii) are satisfied by the orthogonal complements of these hyperbolic planes in L and K respectively. We can therefore assume that L and K do not both contain hyperbolic planes. In particular, we can assume that $1 < \dim L = \dim K \leqq 4$, since the proof of the 1-dimensional case is obvious, while any unitary lattice with dimension $\geqq 5$ must contain at least one hyperbolic plane. We can also suppose that $|\mathfrak{p}| < |\pi^v|$; for the case $\mathfrak{p} = \pi^v\mathfrak{o}$ follows immediately from (12)-(14).

Let us express L in a canonical basis. We can vary modulo $\mathfrak{p}$ a certain diagonal entry in the corresponding matrix for L to obtain a new lattice $L^* \cong L \bmod \mathfrak{p}$ for which $d(L^*) \cong d(K)$. It follows from the necessity of this theorem, already established, that L^* and K continue to satisfy the given conditions. In effect this means that we can take $d(L) \cong d(K)$ from the start.

Case 1. $|\mathfrak{p}| < |4\pi^{-v}$. Since $d(L) \cong d(K)$, the second condition implies that $S(L) = S(K)$, and so L and K are field equivalent by Satz 17 in [WI]. In order to prove that $L \cong K$, we adjoin hyperbolic planes to L and K until we get two corresponding big lattices L' and K'. Then L' and K' are field equivalent, and they represent the same numbers by Proposition 5; hence $L' \cong K'$ by Theorem 19.1 of [OI]; hence $L \cong K$ by Proposition 3.

Case 2. $|\mathfrak{p}| \geqq |4\pi^{-v}|$. If $\dim L = 2$, since $|\pi^v| > |2|$ we can write

$$L \cong \begin{pmatrix} \epsilon\pi^u & 1 \\ 1 & \alpha\pi^v \end{pmatrix}, \qquad |\epsilon| = 1, |\alpha| = 1.$$

Then it is easy to see that K represents $\epsilon\pi^u \bmod 4\pi^{-v}$, hence $\bmod \mathfrak{p}$. We can therefore find a $K^* \cong K \bmod \mathfrak{p}$ such that K^* represents $\epsilon\pi^u$ and $d(L) \cong d(K^*)$. But such a K^* is isometric to L by Theorem 14.3 in [OI]. Hence $L \cong K \bmod \mathfrak{p}$.

If $\dim L = 3$, by (12)-(14) we can write

$$K \cong \begin{pmatrix} \pi^v & 1 \\ 1 & \{4\pi^{-v}\} \end{pmatrix} \oplus \epsilon, \qquad L \cong \begin{pmatrix} \pi^v & 1 \\ 1 & \{4\pi^{-v}\} \end{pmatrix} \oplus \delta$$

where ϵ and δ are units. The result is then immediate since $|\mathfrak{p}| \geqq |4\pi^{-v}|$ and since by a determinantal consideration $\epsilon \cong \delta \bmod \mathfrak{p}$.

Now consider the 4-dimensional case. u and v are of opposite parity since $|4\pi^{-v}| \leqq |\mathfrak{p}| < |\pi^v|$. We recall that we are taking $d(L) \cong d(K)$. By (30) we have $S(L)S(K) = (1 + 4E, \pi)$ for some $E \in \mathfrak{o}$. Write

$$K \cong \begin{pmatrix} \pi^v & 1 \\ 1 & 4\alpha\pi^{-v} \end{pmatrix} \oplus \begin{pmatrix} \epsilon\pi^u & 1 \\ 1 & \beta\pi^r \end{pmatrix}$$

with ϵ a unit, α and β integral. Now consider

$$K^* \cong \begin{pmatrix} \pi^v & 1 \\ 1 & 4\alpha\pi^{-v} - 4E\pi^{-v} \end{pmatrix} \oplus \begin{pmatrix} \epsilon\pi^u & 1 \\ 1 & \beta\pi^v - 4E\epsilon^{-1}\pi^{-u} \end{pmatrix}.$$

Clearly $K^* \cong K \bmod \mathfrak{p}$; and $d(L) \cong d(K^*) \cong d(K)$; computing Hasse symbols we get

$$S(K)S(K^*) = (\epsilon\pi^{u+v}, 1 + 4E) = (\pi, 1 + 4E),$$

using the fact that u and v have opposite parity. Hence $S(K^*) = S(L)$. Adjoining hyperbolic planes to L and K^* we get two lattices which are field equivalent and represent the same numbers; these lattices are isometric by Theorem 19.1 of [OI]; hence $L \cong K^*$; hence $L \cong K \bmod \mathfrak{p}$. This completes the proof of the theorem.

PROPOSITION 9. *L and K are unitary lattices and $\mathfrak{p}$ is an ideal in $\pi\mathfrak{o}$. If H and H' are unit hyperbolic planes and $H \oplus L \cong H' \oplus K \bmod \mathfrak{p}$, then $L \cong K \bmod \mathfrak{p}$.*

Proof. Suppose that $v = v_L \leqq v_K$. If $|\mathfrak{p}| \geqq |\pi^v|$, express L and K in the bases (12)-(14); then we easily see that $L \cong K \bmod \mathfrak{p}$. Now let $|\mathfrak{p}| < |\pi^v|$. Then all the lattices L, $H \oplus L$, $H' \oplus K$, K, have the same a's and v's. Apply the necessity of Theorem 1 to $H \oplus L$, $H' \oplus K$, then the sufficiency to L and K. q. e. d.

COROLLARY 9. *If L and K both represent the same number a of ordinal $u_L = u_K$, and if $H \cong \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} \cong H'$, then*

$$H \oplus L \cong H' \oplus K \bmod \mathfrak{p} \Longrightarrow L \cong K \bmod \mathfrak{p}.$$

If a is a unit, the result holds for $H \cong (a) \cong H'$.

Proof. Let H have the basis $(\mathfrak{o}y_1 + \mathfrak{o}y_2)$ with $y_1^2 = a$, $y_2^2 = 0$. By the proposition we can assume that L and K are big. Hence we can write

$$L \cong \begin{pmatrix} -a & 1 \\ 1 & 0 \end{pmatrix} \oplus \cdots \text{ in } (\mathfrak{o}x_1 + \mathfrak{o}x_2) \oplus \cdots.$$

Apply $\operatorname{op}(y_1 \to y_1 + x_1)$ and do the same with $H' \oplus K$. Now apply the proposition again. To prove the second half consider $a \oplus -a$ instead of the given H and H'. q. e. d.

7. The invariants. Now we can quickly derive our invariants. If $L = \sum L_\lambda$ is a canonical decomposition we define $\mathcal{L}_j = L_1 \oplus L_2 + \cdots \oplus L_j$

for $1 \leqq j \leqq t$. The $\mathfrak{f}_\lambda$ are defined as in Section 5. The quantities $v(\lambda)$, a_λ, d_λ, appearing below are actually defined by the relations (i) and (ii), while the ideal $\mathfrak{d}_\lambda$ is the type invariant given by $d(\mathcal{L}_\lambda)\mathfrak{o} = \mathfrak{d}_\lambda = d(\mathcal{K}_\lambda)\mathfrak{o}$.

THEOREM 2. *Let L and K be two lattices of the same type and in the same space. Let $L = \sum L_\lambda$ and $K = \sum K_\lambda$ be canonical decompositions of L and K. Then L is isometric to K if and only if the following relations hold for all appropriate λ:*

(i) $$v_L(\lambda) = v(\lambda) = v_K(\lambda), \qquad a_\lambda(L) \cong a_\lambda \cong a_\lambda(K) \bmod \pi^{v(\lambda)},$$

(ii) $$d(\mathcal{L}_\lambda) \cong d_\lambda \cong d(\mathcal{K}_\lambda) \bmod \mathfrak{d}_\lambda \mathfrak{f}_\lambda,$$

(iii) $$|\pi^{v(\lambda+1)}\mathfrak{f}_\lambda| < |4\pi^{u(\lambda+1)} \Longrightarrow (d(\mathcal{L}_\lambda), a_{\lambda+1}d_\lambda)\,S(\mathcal{L}_\lambda) = (d(\mathcal{K}_\lambda), a_{\lambda+1}d_\lambda)S(\mathcal{K}_\lambda),$$

(iv) $$|\pi^{v(\lambda)}\mathfrak{f}_\lambda| < |4\pi^{u(\lambda)}| \Longrightarrow (d(\mathcal{L}_\lambda), a_\lambda d_\lambda)\,S(\mathcal{L}_\lambda) = (d(\mathcal{K}_\lambda), a_\lambda d_\lambda)S(\mathcal{K}_\lambda).$$

Proof. If we adjoin a $\pi^{s(i)}$-hyperbolic plane to L we see that the *type* of L is unchanged and so it follows by inspection that the fundamental invariants a_λ, $v(\lambda)$, $\mathfrak{f}_\lambda$ are the same for the enlarged lattice as they are for L, $1 \leqq \lambda \leqq t$. In particular, if the same hyperbolic plane is adjoined to K it follows that the two new lattices will satisfy the relations (i)-(iv) if and only if L and K do. On the other hand, the enlarged lattices will be isometric if and only if $L \cong K$. Hence it suffices for us to consider big lattices only. Now suppose that $\dim L_j$ is an odd number for a certain j $(1 \leqq j \leqq t)$. Let us adjoin a lattice of type (a_j) to both L and K. Then the enlarged lattices will be isometric if and only if $L \cong K$, in virtue of the cancellation law established in Corollary 3. And it is easily verified that L and K have the same invariants (i)-(iv) if and only if the enlarged lattices do. Combining this with our first remark we see that we can assume that both L and K are big and that their components in any canonical decomposition are of even dimension. We shall assume that this is so.

Necessity. We can take $L = K$. The first result is then immediate. We now fix j $(1 \leqq j \leqq t)$ and we establish (ii) and (iv) for $\lambda = j$. A straightforward computation with the Hasse symbols shows that we can in fact take $s(j) = 0$. Construction: adjoin a lattice of type

$$\begin{pmatrix} a_j & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} \pi^{v(j)} & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} a_{j+1} & \pi^{s(j+1)} \\ \pi^{s(j+1)} & 0 \end{pmatrix} \oplus \begin{pmatrix} \pi^{v(j+1)} & \pi^{s(j+1)} \\ \pi^{s(j+1)} & 0 \end{pmatrix}$$

to L and call the resulting lattice L^*. Then the a_λ and $v(\lambda)$ are the same for L^* as for L, by (19). Hence this is also true for $\mathfrak{f}_\lambda$.

Now we can pass from $\sum L_\lambda$ to $\sum K_\lambda$ by a chain of transformations of the type described in Proposition 8. If we can establish (ii) and (iv) for each member of the chain, then we have established it for the given decompositions in virtue of the transitivity of the relations in question. Now (ii) and (iv) are obviously satisfied by a transformation of the first type since $\mathcal{L}_j$ and $\mathcal{K}_j$ do not change. It therefore suffices for us to prove the result for a transformation of the second type. In effect this allows us to assume that $L_\lambda = K_\lambda$ for $1 \leqq \lambda \leqq j-1$, and so

$$L_j^* \oplus L_{j+1}^* \oplus L_{j+2} \oplus \cdots \oplus L_t = K_j^* \oplus K_{j+1}^* \oplus K_{j+2} \oplus \cdots \oplus K_t.$$

Since the "$\mathfrak{f}_1$" for this lattice is precisely $\mathfrak{f}_j$, it follows from Lemma 1 that

$$(31) \qquad L_j^* \cong K_j^* \bmod \pi^{-u(j)}\mathfrak{f}_j, \qquad d(L_j^*)/d(K_j^*) \cong 1 \bmod \mathfrak{f}_j.$$

The second half of this result shows that $d(\mathcal{L}_j)/d(\mathcal{K}_j) \cong 1 \bmod \mathfrak{f}_j$, and so (ii) is established.

We now take d_j as defined by (ii) and we prove (iv). We assume that the condition $|\pi^{v(j)}\mathfrak{f}_j| < |4\pi^{u(j)}|$ is in fact satisfied for the j in question. Thus Theorem 1 when applied to (31) gives

$$(d(L_j^*), a_j d(L_j^*))S(L_j^*) = (d(K_j^*), a_j d(L_j^*))S(K_j^*)$$

and so $(d(L_j)d(K_j), a_j d(L_j))S(L_j)S(K_j) = 1$. Hence

$$(d(\mathcal{L}_j), a_j d_j)S(\mathcal{L}_j) \cdot (d(\mathcal{K}_j), a_j d_j)S(\mathcal{K}_j) = (d(L_j)d(K_j), d_j d(\mathcal{L}_j)),$$

and the right hand side of this equation is of the form

$$(1+\{\mathfrak{f}_j\}, 1+\{\mathfrak{f}_j\}) = (1+\{2\}, 1+\{2\pi\}),$$

which is equal to 1 by (29). This proves (iv).

We now prove (iii). Let $V(\lambda)$, A_λ, $\mathfrak{f}_\lambda^*$ denote the invariants under discussion when evaluated for $\mathfrak{R}L$. We have

$$V(t-\lambda+1) = v(\lambda) - 2s(\lambda), \qquad A_{t-\lambda+1} = a_\lambda \pi^{-2s(\lambda)}, \qquad \mathfrak{f}_{t-\lambda}^* = \mathfrak{f}_\lambda.$$

If we define $\mathcal{L}_\lambda^*$ as the sum of the first λ components in $\mathfrak{R}L = \mathfrak{R}L_t \oplus \cdots \oplus \mathfrak{R}L_1$, we see that $d(\mathcal{L}_\lambda^*) = \alpha^2 d(\mathcal{L}_{t-\lambda})d(L)$ where α is a certain field element. We put $d_\lambda^* = \alpha^2 d_{t-\lambda} d(L)$ and get

$$d(\mathcal{L}_\lambda^*) \cong d_\lambda^* \cong d(\mathcal{K}_\lambda^*) \quad \bmod d_\lambda^* \mathfrak{f}_\lambda^*.$$

Now suppose that condition (iii) is non-vacuous: then $|\pi^{v(j+1)}\mathfrak{f}_j| < |4\pi^{u(j+1)}|$.

Hence $|\pi^{V(t-j)}\mathfrak{f}_{t-j}{}^*| < |4\pi^{U(t-j)}|$. Apply condition (iv) (already proved) to $\mathfrak{R}L$ and we get

$$(d(\mathcal{L}_{t-j}{}^*), A_{t-j}d_{t-j}{}^*)S(\mathcal{L}_{t-j}{}^*) = (d(\mathcal{K}_{t-j}{}^*), A_{t-j}d_{t-j}{}^*)S(\mathcal{K}_{t-j}{}^*).$$

If we resubstitute in this equation, and use the fact that $d(\mathcal{L}_j)/d(\mathcal{K}_j) \cong 1 \bmod 2\pi$, we arrive at condition (iii). This completes the proof of the necessity.

Sufficiency. We are given that (i)-(iv) hold for the particular decompositions $\sum L_\lambda$, $\sum K_\lambda$. In virtue of the necessity (already proved) these conditions must hold for *any* two decompositions $L = \sum L_\lambda$, $K = \sum K_\lambda$. So we can assume that the given decompositions $\sum L_\lambda$, $\sum K_\lambda$ are supersaturated.

We shall prove the sufficiency by an induction on the *length* $s(t) - s(1)$ of L. That the induction can be made to start with lattices of zero length can be seen as follows: since L and K are big, condition (i) implies that they represent the same numbers, and so $L \cong K$ by Theorem 19.1 of [OI]. We note that (ii)-(iv) are vacuous for lattices of zero length. If we now proceed with the induction, it is easy to see that the given conditions are unaltered if we replace L and K by $\pi^k \circ L$ and $\pi^k \circ K$, and so we can take $s(1) = 0$. Since any unitary lattice of dimension $\geqq 5$ contains a hyperbolic plane, we can assume that $\dim L_1 = 4 = \dim K_1$. The basis of the inductive proof will be this: we must find decompositions $L = L_1' \oplus L'$, $K = K_1' \oplus K'$ with

$$L' = L_2' \oplus L_3 \oplus \cdots \oplus L_t, \qquad K' = K_2' \oplus K_3 \oplus \cdots \oplus K_t,$$

where $L_1' \cong K_1'$, and such that L_2', K_2' are still supersaturated components. Once such a reduction has been achieved, it is easy to see that L' and K' will also satisfy the conditions of the theorem. In point of fact, the quantities a_j, $v(j)$, $\mathfrak{f}_j$ are the same for L', K' as for L, K, only a simple relabelling being required. If d_j' is defined by $d_j' = d_j/d(L_1')$, the remaining conditions of the theorem must hold for L' and K'. For the rest of the proof call a saturated decomposition of the given L, supersaturated if the first component represents a number of ordinal $v(1)$ while the remaining components are supersaturated. Similarly with the given K.

One further observation before we start the proof proper. If the supersaturated decompositions $\sum L_\lambda$, $\sum K_\lambda$ are such that $u(1)$ and $u(2)$ have the same parity and if $L_1 \cong K_1 \bmod \pi^{v(2)}$, then we can write $K_1 \oplus K_2$ in a new supersaturated decomposition

$$\bar{K}_1 \oplus \bar{K}_2 = K_1 \oplus K_2 \tag{32}$$

with $L_1 \cong K_1$. We prove this by writing L_1 and K_1 in the canonical bases $\mathfrak{o}x_1 + \mathfrak{o}x_2 + \mathfrak{o}x_3 + \mathfrak{o}x_4$ and $\mathfrak{o}y_1 + \mathfrak{o}y_2 + \mathfrak{o}y_3 + \mathfrak{o}y_4$ respectively, with $x_\lambda^2 = y_\lambda^2 + \alpha_\lambda$ where $\alpha_\lambda \in \pi^{r(2)}\mathfrak{o}$. Since K_2 represents α_λ, we can use Proposition 6 to express

$$K_2 \cong \begin{pmatrix} \alpha_\lambda & \pi^{s(2)} \\ \pi^{s(2)} & 0 \end{pmatrix} \oplus \cdots;$$

where the second component in the above isometry still represents the entire group $a_2\mathfrak{o}^2 + \pi^{v(2)}\mathfrak{o}$. Now apply op$(y_\lambda \to y_\lambda + y_5)$ to get a new K_1 with $x_\lambda^2 = y_\lambda^2$. Doing this for $\lambda = 1, 2, 3, 4$ gives the desired result (32).

Case 1. $u(2) = u(1)$. The first component cannot therefore be proper. Consider $L = \sum L_\lambda$. Since L_2 represents $[\pi^{u(1)}]$, we can use Proposition 6 to apply successive changes of basis to L until we find a decomposition $L = L_1' \oplus L_2' \oplus L_3 \oplus \cdots \oplus L_t$ in which L_2' is still supersaturated, and such that

$$L_1' \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} \pi^{v(1)} & 1 \\ 1 & 4\alpha\pi^{-v(1)} \end{pmatrix},$$

where $\alpha = 0$ when $u(1)$ and $v(1)$ have the same parity or when $|\pi^{v(2)}| \geqq |4\pi^{-v(1)}|$. This construction uses the "op" transformations mentioned in (11) and is similar to the construction used in Lemma 16.3 of [OI]. We omit the details.

We repeat the construction on $K = \sum K_\lambda$. If $u(1)$ and $v(1)$ have the same parity, or if $|\pi^{v(2)}| \geqq |4\pi^{-v(1)}|$, then $L_1' \cong K_1'$ and so

$$L_2' \oplus L_3 \oplus \cdots \oplus L_t \cong K_2' \oplus K_3 \oplus \cdots \oplus K_t$$

by the inductive assumption. We can therefore assume that $u(1) + v(1)$ is odd, $|\pi^{v(2)}| < |4\pi^{-v(1)}|$,

$$(33) \quad L_1' \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} \pi^{v(1)} & 1 \\ 1 & 4\alpha\pi^{-v(1)} \end{pmatrix}, \quad K_1' \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} \pi^{v(1)} & 1 \\ 1 & 4\beta\pi^{-v(1)} \end{pmatrix}.$$

By (23) we have $\mathfrak{f}_1 = \pi^{u(1)+v(1)}\mathfrak{o}$. Then $|\pi^{v(2)}\mathfrak{f}_1| = |\pi^{v(2)+u(1)+v(1)}| < |4\pi^{u(1)}| = |4\pi^{u(2)}|$. Then (iii) must hold for these decompositions of L and K, i.e.

$$(d(L_1'), a_2d_1)S(L_1') = (d(K_1'), a_2d_1)S(K_1'),$$

and so $((1 - 4\alpha)(1 - 4\beta), a_2d_1\pi^{v(1)}) = 1$. Using (28) this implies that $(1 - 4\alpha) \cong (1 - 4\beta)$ and so $L_1' \cong K_1'$. Again we can apply the induction. This completes the first case.

Case 2. $u(2) = u(1) + 1$. Applying a little extra care when $u(1) = 0$, we can proceed as in Case 1 to get decompositions in which

$$(34) \qquad L_1' \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} a_1 & 1 \\ 1 & 4\alpha\pi^{-u(1)} \end{pmatrix}, \quad K_1' \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} a_1 & 1 \\ 1 & 4\beta\pi^{-u(1)} \end{pmatrix},$$

where $\alpha = \beta = 0$ when $|\pi^{v(2)}| \geqq |4\pi^{-u(1)}|$. So we consider $|\pi^{v(2)}| < |4\pi^{-u(1)}|$. Then $|\pi^{v(2)}\mathfrak{f}_1| = |\pi^{v(2)+u(1)+u(2)}| < |4\pi^{u(2)}|$. Condition (iii) again gives $L_1' \cong K_1'$. Thus Case 2 is established.

Case 3. $u(1) = e$. In virtue of Cases 1 and 2, we can assume that $|\pi^{u(2)}| \leqq |\pi^{u(1)+2}| = |2\pi^2|$. Then we easily see that $|\mathfrak{f}_1| \leqq |4\pi|$. Now

$$L_1 \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 2 & 1 \\ 1 & \{2\} \end{pmatrix}, \qquad K_1 \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 2 & 1 \\ 1 & \{2\} \end{pmatrix}.$$

But $d(L_1) \cong d(K_1) \bmod 4\pi$. Hence $L_1 \cong K_1$. So this case is proved.

Case 4. $s(2) = s(1) + 1$. Then in virtue of the first three cases we can take $u(1) < e$, $u(2) = u(1) + 2$. Also $s(1)$ is assumed to be 0, and so $s(2) = 1$. Then the behaviour of $v(1)$ and $v(2)$ can affect our result in three different ways. In the first place, we may have $|\pi^{v(1)}| > |2|$, and so $|\pi^{v(2)}| \geqq |\pi^{v(1)+2}|$. Then by (25) we have $\mathfrak{f}_1 = \pi^{v(2)+u(1)}\mathfrak{o}$, hence $d(L_1) \cong d(K_1) \bmod \pi^{v(2)+u(1)}$. But $|\pi^{v(2)}| \geqq |\pi^{v(1)+2}| \geqq |4\pi^{-v(1)}|$, since $|\pi^{v(1)}| > |2|$. Hence $L_1 \cong K_1 \bmod \pi^{v(2)}$ by Theorem 1. We can therefore write K in the supersaturated decomposition $K = K_1' \oplus K_2' \oplus K_3 \oplus \cdots \oplus K_t$ in which $L_1 \cong K_1'$. We then use the inductive hypothesis to arrive at the isometry $L \cong K$. In the second place, we may have $v(1) = e = v(2)$. Then obviously $L_1 \cong K_1 \bmod 2$. Hence we can find a supersaturated decomposition $K = K_1' \oplus K_2' \oplus K_3 \oplus \cdots \oplus K_t$ in which $K_1' \cong L_1$. Again we are through. Thirdly and finally, we may have $v(1) = e < v(2)$; then in fact $v(2) = e + 1$. Since $\mathfrak{f}_1 = 2\pi^{u(1)+1}\mathfrak{o}$, $\pi^{v(1)}\mathfrak{f}_1 = 4\pi \cdot \pi^{u(1)}\mathfrak{o}$, condition (iv) must be non-vacuous and we get

$$(d(L_1), a_1 d_1) S(L_1) = (d(K_1), a_1 d_1) S(K_1).$$

Thus $L_1 \cong K_1 \bmod 2\pi$ by Theorem 1. Hence the result follows from (32).

Case 5. $s(2) > s(1) + 1$. We can take $u(1) < e$, $u(2) \geqq u(1) + 2$. Define N_* as the orthogonal sum of six π^1-hyperbolic planes and let L^* and K^* be defined by the canonical decompositions

$$L^* = L_1 \oplus N_* \oplus L_2 \oplus \cdots \oplus L_t, \qquad K^* = K_1 \oplus N_* \oplus K_2 \oplus \cdots \oplus K_t.$$

Now it follows immediately from the definition of the quantities involved that $u^*(j) = u(j)$, $v^*(j) = v(j)$, $a_j^* = a_j$ for $j = 1, 2, 3, \cdots, t$. Hence

$$(35) \qquad \mathfrak{f}_j^* = \mathfrak{f}_j \qquad \text{for } j = 2, 3, 4, \cdots, t.$$

All these quantities are clearly the same for L^* as for K^*. We agree to drop the *'s except for emphasis. Notice that the notation has suffered a minor inconsistency in passing from L to L^*. Thus $a_1{}^*$ and $v^*(1)$ still refer to $L_{(0)}{}^*$. But for $j \geqq 2$ we are now using $a_j{}^*$ and $v^*(j)$ to describe $L_{(s(j))}{}^*$, although strictly speaking they should be relabelled $a_{j+1}{}^*$ and $v^*(j+1)$ with j running from 0 to t. Similar remarks apply to $\mathfrak{f}_j{}^*$. We shall use a_* and $v(*)$ to describe the numbers represented by $L_{(1)}{}^*$.

How are a_*, $v(*)$, $\mathfrak{f}_1{}^*$, and $\mathfrak{f}_*{}^* = \mathfrak{f}_*$ related? Since $u(*) = u(1) + 2$, we can take $a_* = a_1\pi^2$. We also have

$$v(1) \leqq v(*) \leqq v(1) + 2, \qquad v(*) \leqq e + 1.$$

Note that $L_{(1)}{}^*$ and $K_{(1)}{}^*$ represent the same numbers and so $v(*)$ is the same for both. If we choose a semi-canonical basis $\langle x \rangle$ corresponding to the supersaturated decomposition $\sum L_\lambda$ in which L_1 and L_2 both have the form (12)-(14), we easily see from (21) that

$$\text{(36)} \qquad \mathfrak{f}_1{}^* \supseteqq \mathfrak{f}_1, \qquad \mathfrak{f}_* \supseteqq \mathfrak{f}_1.$$

Let us consider the invariants of L^* and K^*. We put $d_1{}^* = d_1$, $d_* = \pi^{12} d_1$, $d_\lambda{}^* = \pi^{12} d_\lambda$ for $2 \leqq \lambda \leqq t$. Then condition (i) holds between L^* and K^* for all λ. By (35) and (36) we see that for $\lambda = 1, *, 2, 3, \cdots, t$,

$$d(\mathcal{L}_\lambda{}^*) \cong d_\lambda{}^* \cong d(\mathcal{K}_\lambda{}^*) \bmod \mathfrak{f}_\lambda{}^* d_\lambda{}^*.$$

Now consider (iv) for the two enlarged lattices. If we have $|\pi^{v(1)}\mathfrak{f}_1{}^*| < |4\pi^{u(1)}|$, then $|\pi^{v(1)}\mathfrak{f}_1| < |4\pi^{u(1)}|$, in virtue of (36), and so (iv) holds when $\lambda = 1$. If $\lambda = *$, and $|\pi^{v(*)}\mathfrak{f}_*| < |4\pi^{u(*)}|$, then

$$|\pi^{v(1)}\mathfrak{f}_1| \leqq |\pi^{v(*)-2}\,\mathfrak{f}_*| < |4\pi^{u(*)-2}| = |4\pi^{u(1)}|;$$

hence

$$(d(\mathcal{L}_1), a_1 d_1) S(\mathcal{L}_1) = (d(\mathcal{K}_1), a_1 d_1) S(\mathcal{K}_1)$$

and so

$$(d(\mathcal{L}_*{}^*), a_* d_*) S(\mathcal{L}_*{}^*) = (d(\mathcal{K}_*{}^*), a_* d_*) S(\mathcal{K}_*{}^*).$$

Condition (iv) is immediate for $\lambda = 2, 3, \cdots, t$.

Now consider condition (iii). For $\lambda = 1$, we have $|\pi^{v(*)}\mathfrak{f}_1{}^*| = |\pi^{u(1)+2v(*)}| \geqq |4\pi^{u(*)}|$ since $|\pi^{v(*)}| \geqq |2\pi|$. Thus (iii) is vacuous when $\lambda = 1$. On the other hand it follows from (35) and (36) that (iii) holds when $\lambda = *, 2, 3, \cdots, t$.

We have therefore shown that L^* and K^* satisfy the invariants of the theorem. Now L^* and K^* have length $s(t) - s(1) = s(t)$; and the result has been established for lattices of this length which satisfy $s(2) = s(1) + 1$;

hence $L^* \cong K^*$; hence $L \cong K$ by Proposition 3. This completes the proof of Theorem 2.

Condition (ii) of Theorem 2 gives a determinantal description of how $\mathscr{L}_j$ varies as we change the canonical decomposition $L = \sum L_\lambda$ of L. If we define

$$\mathfrak{b}_1 = \pi^{2s(1)-u(1)}\mathfrak{f}_1, \qquad \mathfrak{b}_j = \pi^{2s(j)-u(j)}(\mathfrak{f}_{j-1} + \mathfrak{f}_j), \qquad \mathfrak{b}_t = \pi^{2s(t)-u(t)}\mathfrak{f}_{t-1}.$$

we shall see that these quantities describe the change in the j-th component of $\sum L_\lambda$. Note that $\mathfrak{b}_j(\alpha \circ L) = \alpha \mathfrak{b}_j(L)$.

THEOREM 3. *$\sum L_\lambda = L = \sum K_\lambda$ are two saturated canonical decompositions of L. Then $L_j \cong K_j \bmod \mathfrak{b}_j$ for $1 \leqq j \leqq t$.*

Proof. In virtue of Proposition 9 we can assume that L is a big lattice. It suffices to prove the result when $s(j) = 0$ and when one of the decompositions, let us say $\sum L_\lambda$, is supersaturated. Let a_j be represented by K_j; then it is represented by L_j since $\sum L_\lambda$ is supersaturated. So we can assume that $\dim L_j$ is even, by Corollary 9. If $j = 1$ we have $L_1 \cong K_1 \bmod \mathfrak{b}_1$ by Lemma 1. If $j = t$ the result follows by considering $\mathfrak{R}L$ instead of L.

Now suppose that $1 < j < t$. Adjoin

$$\begin{pmatrix} a_{j-1} & \pi^{s(j-1)} \\ \pi^{s(j-1)} & 0 \end{pmatrix} \oplus \begin{pmatrix} a_j & \pi^{s(j)} \\ \pi^{s(j)} & 0 \end{pmatrix} \oplus \begin{pmatrix} a_{j+1} & \pi^{s(j+1)} \\ \pi^{s(j+1)} & 0 \end{pmatrix}$$

to L and call the new lattice L^*. Then we can pass from $\sum L_\lambda^*$ to $\sum K_\lambda^*$ through a chain of transformations

$$\sum L_\lambda^* \to \cdots \to \sum I_\lambda^* \to \sum J_\lambda^* \to \cdots \to \sum K_\lambda^*$$

such that each I_λ^* represents $a_\lambda (j-1 \leqq \lambda \leqq j+1)$ and such that either $\sum_j^t I_\lambda^* = \sum_j^t J_\lambda^*$ or $\sum_1^j I_\lambda^* = \sum_1^j J_\lambda^*$. If the transformation is of the first type we have $I_j^* \cong J_j^* \bmod \mathfrak{b}_j$ by Lemma 1, since $\mathfrak{f}_1(\sum_j^t L_\lambda^*) \subseteq \mathfrak{f}_j \subseteq \pi^{u(j)}\mathfrak{b}_j$. If the transformation is of the second type we can deal with $\mathfrak{R}L^*$ instead of L^* and we again get $I_j^* \cong J_j^* \bmod \mathfrak{b}_j$. Hence $L_j^* \cong K_j^* \bmod \mathfrak{b}_j$. Hence $L_j \cong K_j \bmod \mathfrak{b}_j$ by Corollary 9. q.e.d.

8. Concluding remarks. Our main result, Theorem 2, expresses the invariants of L in terms of the fundamental invariants a_j and $v(j)$ which were derived from the simplest invariant substructures of L. We now show that the numerical computation of these quantities can be reduced to the field problem of computing quadratic residues.

Since we can express L in a canonical basis using elementary operations only, we suppose that L is expressed in a semi-canonical basis $\sum \mathfrak{o}x_\lambda$. Write $t(\lambda) = \operatorname{ord} x_\lambda \cdot L$. Then $t(1) \leqq t(2) \leqq \cdots \leqq t(n)$. The basis $\langle x \rangle$ induces a canonical decomposition $L = \sum L_\lambda$ on L where the $s(j)$'s and $t(\lambda)$'s have the same range of values. Now we can easily define a_j: a_j is the greatest of the field elements

$$\pi^{2s(j)-2t(\lambda)}x_\lambda^2, \quad x_\gamma^2, \quad 2\pi^{s(j)}$$

under the given valuation, where x_λ runs through $L_1 \oplus \cdots \oplus L_{j-1}$ and x_γ runs through $L_j \oplus \cdots \oplus L_t$.

Suppose that all a_j have been determined. *Contention*:

$$(37) \qquad \pi^{v(j)}\mathfrak{o} = \sum \pi^{2s(j)-2t(\lambda)}x_\lambda^2\mathfrak{g}(a_jx_\lambda^2) + \sum x_\gamma^2\mathfrak{g}(a_jx_\gamma^2) + 2\pi^{s(j)}\mathfrak{o},$$

where x_λ runs through $L_1 \oplus \cdots \oplus L_{j-1}$ and x_γ runs through $L_j \oplus \cdots \oplus L_t$.

Proof of contention. We write $\pi^\mu\mathfrak{o}$ for the ideal defined in (37). We must prove that $\mu = v(j)$. We can take $s(j) = 0$. If we consider $\mathfrak{P}L$ we see that $\mu_L(j) = \mu_{\mathfrak{P}L}(1)$, while $v_L(j) = v_{\mathfrak{P}L}(1)$ by definition of $v(j)$. Thus we can assume that $j = 1$ and $s(1) = 0$. We must therefore prove that $v(1) = \mu$ where

$$\pi^\mu\mathfrak{o} = \sum x_\gamma^2\mathfrak{g}(a_1x_\gamma^2) + 2\mathfrak{o}.$$

First we prove $|\pi^{v(1)}| \geqq |\pi^\mu|$. This clearly holds if $\mu = e$; hence we assume that $\mu < e$, hence $\pi^\mu\mathfrak{o} = x_i^2\mathfrak{g}(a_1x_i^2)$ for some i. If $x_i^2 \in \pi^{v(1)}\mathfrak{o}$, we are through. Hence suppose that $x_i^2 = a_1\alpha^2 + \{\pi^{v(1)}\}$ with $|a_1\alpha^2| > |\pi^{v(1)}|$. Then

$$\pi^\mu\mathfrak{o} = \alpha^2a_1\mathfrak{g}(1 + \{\alpha^{-2}a_1^{-1}\pi^{v(1)}\}) \subseteq \pi^{v(1)}\mathfrak{o}.$$

Conversely we prove $|\pi^{v(1)}| \leqq |\pi^\mu|$. Suppose if possible that $|\pi^{v(1)}| > |\pi^\mu|$. So $|\pi^{v(1)}| > |2|$. Then we must have $x_\lambda^2 = \alpha_\lambda^2a_1 + \beta_\lambda\pi^{v(1)+1}$ for all λ. Now any $x \in L$ can be written $\sum c_\lambda x_\lambda$. Then

$$x^2 \equiv \sum \alpha_\lambda^2c_\lambda^2a_1 \equiv (\sum \alpha_\lambda c_\lambda)^2a_1 \bmod \pi^{v(1)+1}.$$

In particular, this is true for a vector x whose norm has ordinal $v(1)$. This is impossible since $v(1)$ and $u(1)$ have opposite parity when $|\pi^{v(1)}| > |2|$. q. e. d.

Let us call a big lattice L *dense* if $s(\lambda + 1) = s(\lambda) + 1$ for $1 \leqq \lambda \leqq t - 1$. Then in virtue of Proposition 3 the problem of this paper is equivalent to the problem of finding when two dense lattices L and K are equivalent. It is worth noting that the results can be simplified if we restrict ourselves to dense lattices only. Thus the u's will satisfy (22); the $\mathfrak{f}$'s are given by

(23)-(25); and Theorem 2 can be established without considering Case 5 in the proof of the sufficiency.

We conclude by giving a counter-example to show that both the conditions (iii) and (iv) are required in our characterization. Let F be the field $R_2(\pi)$ where R_2 is the 2-adic numbers and π is a root of $x^8 - 2 = 0$. For any $E \in \mathfrak{o}$ define L as the lattice with associated matrix

$$\begin{pmatrix} \pi & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 2 & 1 \\ 1 & 2E \end{pmatrix} \oplus \begin{pmatrix} \pi^3 & \pi \\ \pi & 0 \end{pmatrix} \oplus \begin{pmatrix} \pi^5 & \pi^2 \\ \pi^2 & 0 \end{pmatrix} \oplus \begin{pmatrix} 2\pi^2 & \pi^2 \\ \pi^2 & 2\pi^2 E \end{pmatrix}.$$

Let K be given by the same matrix, but with $E = 0$. We can suppose that the E in L is a unit for which $(1 - 4E, \pi) \neq 1$. For both L and K we have

$$a_1 = \pi, \quad a_2 = \pi^3, \quad a_3 = \pi^5, \quad v(1) = e, \quad v(2) = e + 1, \quad v(3) = e + 2$$

$$\mathfrak{f}_1 = 2\pi^2 \mathfrak{o}, \quad \mathfrak{f}_2 = 2\pi^3 \mathfrak{o}.$$

We see that (i)-(ii) hold for L and K. Also (iii) is satisfied, being vacuous. But (iv) does not hold. Hence by the necessity of Theorem 2. L and K cannot be isometric.

UNIVERSITY OF OTAGO,
NEW ZEALAND.

REFERENCES.

[AI] E. Artin, "Algebraic numbers and algebraic functions I," *Princeton University, New York University*, 1950-1951.

[AsI] K. Asano, "Über Moduln und Elementarteilertheorie im Körper, in dem Arithmetik definiert ist," *Japanese Journal of Mathematics*, vol. 20 (1950), pp. 55-71.

[DI] W. H. Durfee, "Congruence of quadratic forms over valuation rings," *Duke Mathematical Journal*, vol. 11 (1944), pp. 687-697.

[EI] M. Eichler, *Quadratische Formen und orthogonale Gruppen*, Berlin (1952).

[JI] B. W. Jones; "A canonical quadratic form for the ring of 2-adic integers," *Duke Mathematical Journal*, vol. 11 (1944), pp. 715-727.

[JII] ———, "The arithmetic theory of quadratic forms," *Carus Monographs*, No. 10, Mathematical Association of America, 1950.

[OI] O. T. O'Meara, "Quadratic forms over local fields," *American Journal of Mathematics*, vol. 77 (1955), pp. 87-116.

[OII] ———, "Witt's theorem and the isometry of lattices," *Proceedings of the American Mathematical Society*, vol. 7 (1956), pp. 9-22.

[PI] G. Pall, "The arithmetical invariants of quadratic forms," *Bulletin of the American Mathematical Society*, vol. 51 (1945), pp. 185-197.

[WI] E. Witt, "Theorie der quadratischen Formen in beliebigen Körpern," *Journal für die reine und angewandte Mathematik*, vol. 176 (1937), pp. 31-44.

ON JACOBI BRACKETS.*

By Philip Hartman.

Hypothesis (H): Let $z = z(x)$ be a solution of the pair of partial differential equations

$$(1_F) \qquad F(x,p,z) = 0, \qquad\qquad (1_G) \qquad G(x,p,z) = 0,$$

where z, F, G are scalar functions of class C^1 of their arguments,

$$x = (x^1, \cdots, x^n), \qquad p = (p^1, \cdots, p^n),$$

and $p = \operatorname{grad} z$ in (1).

A standard theorem states that if (H) holds and if z is of class C^2 (instead of merely C^1), then z is a solution of the partial differential equation

$$(2) \qquad [F, G] = 0,$$

where $[F, G]$, the Jacobi bracket, is the function of (x, z, p) defined by

$$(3) \qquad [F, G] = \sum_{k=1}^{n} (F_k(G^k + p^k G_z) - G_k(F^k + p^k F_z))$$

in terms of $F_k = \partial F/\partial p^k$, $F^k = \partial F/\partial x^k$ and the corresponding partial derivatives of G.

If F and G are linear in the components of p, then the additional assumption that z is of class C^2 is not needed in this assertion; cf. the results on Poisson parenthesis in Ostrowski [1] and the references there to Gillis, E. Schmidt and Perron.

Professor Wintner has raised the question whether or not the additional assumption that z is of class C^2 can be omitted in the general (non-linear) case. In this note, his question will be answered in the affirmative if $n = 2$ and, under an additional condition, if $n > 2$. For example, if $n \geqq 2$ and if one of the functions F or G is linear in the components of p, then the answer is in the affirmative; in particular, there will result a new simple proof for the case that both F and G are linear in the components of p.

The results will be obtained as corollaries of the theorems of Pliś [2]

---

* Received May 23, 1956.

on the existence of characteristics on a solution of a partial differential equation. His theorems are applicable by virtue of the following remark:

(*) Assume hypothesis (H). Suppose that, on some t-interval, $(x, p, z) = (x(t), p(t), z(t))$ is a solution of the system of differential equations for characteristics

$$x^{k\prime} = F_k(x, p, z), \qquad p^{k\prime} = -F^k(x, p, z) - p^k F_z(x, p, z), \tag{4}$$
$$z' = \sum_{k=1}^{n} p^k F_k(x, p, z),$$

where $' = d/dt$, and that $z(t) = z(x(t)), p(t) = \operatorname{grad} z(x(t))$. Then the relation (2) holds for $(x, p, z) = (x(t), p(t), z(t))$.

In order to verify this, note that $G(x(t), p(t), z(t)) = 0$, since z is a solution of (1_G). Differentiation of this relation $G = 0$ with respect to t is permitted and gives $\sum(G^k x^{k\prime} + G_k p^{k\prime}) + G_z z' = 0$. In view of (3), the relation (2) for $(x, p, z) = (x(t), p(t), z(t))$ follows from (4).

(i) Assume hypothesis (H) and $n = 2$. Then (2) holds for $(x, p, z) = (x, \operatorname{grad} z(x), z(x))$.

For convenience, let (x, y) and (p, q) be used instead of the vector notation x and p. The relation (2) holds at a point (x, y, p, q, z) if $F_p = F_q = G_p = G_q = 0$. Suppose that, at some point, say

$$(x, y, p, q, z) = (0, 0, p(0,0), q(0,0), z(0,0)),$$

one of these partial derivatives, say F_p, is not 0. Then, in some neighborhood of that point, the partial differential equation $F = 0$ can be written in the form

$$p = f(x, y, z, q), \tag{5}$$

where f is of class C^1 in its arguments. Also, (4) is equivalent to the system

$$y' = -f_q, \qquad z' = f - qf_q, \qquad q' = f_y + qf_z, \qquad p' = f_x + pf_z, \tag{6}$$

where $' = d/dx$. According to Pliś [2], there exist for small $|x|$ (continuously differentiable) functions $y = y(x)$, $z = z(x)$, $q = q(x)$ satisfying the first three equations in (6) and the conditions $y(0) = 0$, $z(x) = z(x, y(x))$, $q(x) = z_y(x, y(x))$. It follows from (5) that $p(x) = z_x(x, y(x))$ has a continuous derivative $p'(x)$ and that the last equation in (6) is a consequence of the first three and of (5). Thus (i) follows from (*).

(ii) Assume hypothesis (H) and $n > 2$. Then (2) holds for $(x, p, z) = (x, \operatorname{grad} z(x), z(x))$ if the initial value problem

$$dx^k/dt = F_k(x, \operatorname{grad} z(x), z(x)), \qquad x(0) = x_0 \tag{7}$$

has a unique (local) solution for every point $x = x_0$ with the property that at least one of the partial derivatives $F_k = \partial F/\partial p^k$, where $k = 1, \cdots, n$, is not 0 at $(x, p, z) = (x_0, \operatorname{grad} z(x_0), z(x_0))$.

This follows from the above arguments and from a theorem of Pliś [2] concerning existence of characteristics on C^1-solutions of equations (5), where x, p, z are scalars, $y = (y^1, \cdots, y^n)$ and $q = (q^1, \cdots, q^n)$, $q^k = \partial z/\partial y^k$.

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES

[1] A. Ostrowski, " Sur un théorème fondamental de la théorie des équations linéaires aux dérivées partielles," *Commentarii Mathematici Helvetici*, vol. 15 (1942/43), pp. 217-221.

[2] A. Pliś, " Characteristics of non-linear partial differential equations," *Bulletin de l'Académie Polonaise des Sciences*, Cl. III, vol. 2 (1954), pp. 419-422.

ON THE FINITE FACTOR GROUPS OF ABELIAN GROUPS OF FINITE RATIONAL RANK.*

By SHREERAM ABHYANKAR.

1. Introduction. In our recent paper we have given a proposition (Proposition 1 of Section 3 of [2]) to the effect that a finite factor group of a torsion free abelian group of rational rank one is necessarily cyclic. In the present paper we generalize this result to groups of finite rational rank, namely, we shall prove the following theorem.

THEOREM. *Let A be a torsion free abelian group of finite rational rank n and let B be a proper subgroup of A of finite index. Then A/B is a direct sum of m cyclic groups with $m \leqq n$.*

From this theorem, in view of Satz 3 of Krull [4] and Theorem 1 of [5], we obtain the following corollary.

COROLLARY. *Let K be an n-dimensional algebraic function field over an algebraically closed ground field k of characteristic zero, and let K^* be a galois extension of K. Let v^* be a real zero-dimensional valuation of K^*/k and let v be the K-restriction of v^*. Then the splitting group of v^* over v is a direct sum of m cyclic groups with $m \leqq n$.*

Now let us refer to the discussion of the resolution problem sandwiched between Theorems 2A and 9A of Section 9 of our paper [2]. There we raised a valuation-ramification theortic objection to Theorem Z, which leads us to conclude that Theorem Z must be weakened at least to the point as to read: . . . every singularity of $f[V_r]$ is an s-fold normal crossing with $s \leqq r+1$. In view of Theorem 2 of [1]. the above corollary says that as far as valuation-ramification theory is concerned, this weakened form of Theorem Z is unobjectionable. This resolution theoretic implication accounts for our interest in the theorem of the present paper.

2. Proof of the theorem. The proof of the theorem will be preceded by two propositions. We shall use the following notations. By R and Z we shall denote respectively the additive groups of the rational numbers and the integers. For a positive integer n, we shall denote by $Z(n)$ a cyclic group of order n. For a prime number p, we shall denote by $Z(p^{\infty})$ the additive

---

* Received May 2, 1956.

group of those rational numbers whose denominators are powers of p. For abelian groups $G, G_1, G_2, \cdots, G_m,$ we shall denote by $\bigoplus_{i=1}^{m} G_i$ and $\bigoplus_{m} G$ respectively the direct sum of $G_1, G_2, \cdots, G_m,$ and the direct sum of m isomorphic copies of G. For well known properties of finite abelian groups which we shall use, we refer to Chapter 3 of [6].

PROPOSITION 1. *Let* $G = \bigoplus_{n} Z(p^\infty)$ *where* p *is a given prime number. Let* A *be a subgroup of* G *and let* B *be a proper subgroup of* A *of finite index. Then* $A/B = \bigoplus_{i=1}^{m} Z(p^{a_i})$ *where the* a_i *are unique integers such that* $1 \leqq a_1 \leqq a_2 \leqq \cdots \leqq a_m$ *and* $m \leqq n$.

Proof. Let G^* (respectively A^*) be the subgroup of elements u in G (respectively in A/B) such that $pu = 0$. Then $G^* = \bigoplus_{n} Z(p)$. Since the order of every element of G is a power of p, the same is true for elements of A/B. Since A/B is finite, we have $A/B = \bigoplus_{i=1}^{m} Z(p^{a_i})$ where the a_i are unique integers such that $1 \leqq a_1 \leqq a_2 \leqq \cdots \leqq a_m$. This direct sum decomposition of A/B implies that $A^* = \bigoplus_{m} Z(p)$. Let f denote the canonical homomorphism of A onto A/B. Let $u_1, u_2, \cdots, u_m$ be a basis of A^* and fix v_i in A such that $f(v_i) = u_i$. Let A_1 be the subgroup of A generated by $v_1, v_2, \cdots, v_m$; let $B_1 = pA_1$, and let $A_1{}^*$ be the subgroup of elements u of A_1 such that $pu = 0$. Then $B_1 \subset (A_1 \cap B)$ and $[A_1 : B_1] \leqq p^m$; since $f(A_1) = A_1/(A_1 \cap B) = A^*$ we must have $[A_1 : B_1] = p^m$ and $B_1 = A_1 \cap B$. Since A_1 is of finite order which is a power of p and since $A_1/B_1 = A^* = \bigoplus_{m} Z(p)$ we conclude that $A_1 = \bigoplus_{i=1}^{m} Z(p^{b_i})$. Therefore $A_1{}^* = \bigoplus_{m} Z(p)$. Since $A_1{}^*$ is a subgroup of G^* we must have $m \leqq n$.

PROPOSITION 2. *Let* $G = \bigoplus_{n} (R/Z)$. *Let* A *be a subgroup of* G *and let* B *be a proper subgroup of* B *of finite index. Then* $A/B = \bigoplus_{i=1}^{m} Z(q_i)$ *with* $m \leqq n$.

Proof. As in the proof of Proposition 1 of [2], $R/Z = \bigoplus_{p \in P} Z(p^\infty)$ where P is the set of all prime numbers. Hence $G = \bigoplus_{p \in P} Z_n(p^\infty)$ where $Z_n(p^\infty) = \bigoplus_{n} Z(p^\infty)$. It is clear that $Z_n(p^\infty)$ is the subgroup of exactly those elements of G whose orders are powers of p. Let A_p and B_p denote the subgroups respectively of A and B consisting of all those elements whose orders are powers of p. By Theorem [1] of [3], we have that $A = \bigoplus_{p \in P} A_p$

and $B = \bigoplus_{p \in P} B_p$. Hence $A/B = \bigoplus_{p \in P} (A_p/B_p)$. By Proposition 1 we have that for a given prime number p either $A_p = B_p$ or

$$A_p/B_p = \bigoplus_{i=1}^{m_p} Z(p^{a_{pi}})$$

with $1 \leqq a_{p1} \leqq a_{p2} \leqq \cdots \leqq a_{pm_p}$ and $m_p \leqq n$. Since A/B is finite, we must have $A_p = B_p$ for all prime numbers p except for a finite number, say $p_1, p_2, \cdots, p_s$. Then

$$A/B = \bigoplus_{i=1}^{s} (A_{p_i}/B_{p_i}).$$

Let $m = \max(m_{p1}, m_{p2}, \cdots, m_{p_s})$ and set $a_{p_ij} = 0$ if $m \geqq j > m_{p_i}$. For $j = 1, 2, \cdots, m$, let

$$q_j = \prod_{i=1}^{s} p_i^{a_{p_ij}}.$$

Then $A/B = \bigoplus_{i=1}^{m} Z(q_i)$, with $m \leqq n$.

Proof of the theorem. Since B is a subgroup of A of finite index, B is also of rational rank n. Let $u_1, u_2, \cdots, u_n$ be a rational basis of B. Then $u_1, u_2, \cdots, u_n$ is a rational basis also of A. Let $G = \bigoplus_n R$. Then there is a unique isomorphism of A into G which maps u_i (for $i = 1, 2, \cdots, n$) onto the element of G all of whose components (in the given direct sum decomposition of G) except the i-th one are zero and whose i-th component in 1. We shall assume that by this isomorpphism A has been identified with a subgroup of G. Let Z_n be the subgroup of G generated by $u_1, u_2, \cdots, u_n$. Let $G^* = G/Z_n$, $A^* = A/Z_n$, and $B^* = B/Z_n$. Then B^* is a proper subgroup of A^*, A^* is a subgroup of G^*, $G^* = \bigoplus_n (R/Z)$, and A/B is isomorphic to A^*/B^*. Now the theorem follows from Proposition 2.

COLUMBIA UNIVERSITY.

REFERENCES.

[1] S. Abhyankar, "On the ramification of algebraic functions," *American Journal of Mathematics*, vol. 77 (1955), pp. 575-592.

[2] ———, "Simultaneous resolution for algebraic surfaces," *American Journal of Mathematics*, vol. 78 (1956), pp. 761-790.

[3] I. Kaplansky, *Infinite abelian groups*, Ann Arbor, 1954.

[4] W. Krull, "Galoische Theorie bewerteter Körper," Sitzungsberichte der Bayerischen Akademie der Wissenschaften, München (1930), pp. 225-238.

[5] S. MacClane and O. F. G. Schilling, "Zero-dimensional branches of rank one on algebraic varieties," *Annals of Mathematics*, vol. 40 (1939), pp. 507-520.

[6] A. Speiser, *Die Theorie der Gruppen*, New York, 1943.

FOURIER TRANSFORMS ON A SEMISIMPLE LIE ALGEBRA I.*

By Harish-Chandra.

1. Introduction. Let $\mathfrak{g}_0$ be a real semisimple Lie algebra and $\mathfrak{h}_0$ a Cartan subalgebra of $\mathfrak{g}_0$. Consider the connected adjoint group G of $\mathfrak{g}_0$ and its Cartan subgroup A corresponding to $\mathfrak{h}_0$ (see [2(e), §2]). Put $G^* = G/A$ and $x^*H = xH$ $(x \in G, H \in \mathfrak{h}_0)$, where $x \to x^*$ is the natural mapping of G on G^*. Let dx^* denote the invariant measure on G^*. Define π as in [2(h), §3] and let $\mathfrak{h}_0'$ be the set of those points $H \in \mathfrak{h}_0$ where $\pi(H) \neq 0$. Then we shall show that the integral

$$\phi_f(H) = \pi(H) \int_{G^*} f(x^*H)\, dx^* \qquad (H \in \mathfrak{h}_0')$$

is convergent for $f \in \mathcal{B}(\mathfrak{g}_0)$ (see [2(h), §2] for the notation used here and below.). Moreover, if $\bar{f}$ denotes the Fourier transform of f, there exists a rather simple relationship between $\phi_{\bar{f}}$ and ϕ_f (see Lemma 24). This fact is the appropriate generalization to the noncompact case of Theorem 3 of [2(h)]. Let $\mathfrak{h}_1$ be a connected component of $\mathfrak{h}_0'$. One of our principal objects is to show that

$$\lim_{H \to 0} \phi_f(H; \partial(\pi)) = cf(0) \qquad (H \in \mathfrak{h}_1, f \in \mathcal{B}(\mathfrak{g}_0)),$$

where c is a complex number independent of f. (This corresponds to Lemma 16 of [2(h)] in the compact case). Actually, it would turn out that $c = 0$ very often. Nevertheless, $\mathfrak{h}_0$ and $\mathfrak{h}_1$ can always be so chosen that $c \neq 0$. (The proof of these statements is rather long and will be completed only in the next paper of this series.) As we shall see in another paper, these results are intimately related to the Plancherel formula for any connected Lie group which is locally isomorphic to G. In the special case of the $n \times n$ real unimodular group, the above expression for $f(0)$ in terms of ϕ_f has been obtained by Gelfand and Graev [1].

CALCU
CENTR
LIBRA
UNIVE

Let $\mathfrak{k}_0$ be the subalgebra of $\mathfrak{g}_0$ corresponding to a maximal compact subgroup K of G. We shall see that for most of our proofs, the crucial case is when $\mathfrak{h}_0 \subset \mathfrak{k}_0$. Lemma 5 contains the fundamental inequalities which

---

* Received July 30, 1956.

allow us to establish the main properties of ϕ_f (see Theorem 2) in this case. In Section 5, we discard the above assumption on $\mathfrak{h}_0$ and extend these results to the general case. The most important one among them is the relation $\phi_{\partial(p)f} = \partial(\bar{p})\phi_f$ $(p \in I(\mathfrak{g}), f \in \mathcal{C}(\mathfrak{g}_0))$ which, in its turn, follows from Theorem 1 of [2(h)]. On the other hand, these differential equations give us the above-mentioned results concerning Fourier transforms (see Section 6).

Select $\mathfrak{h}_0$ and $\mathfrak{h}_1$ as above, and put

$$T'(f) = \lim_{H\to 0} \phi_{\bar{f}}(H;\partial(\pi)) \qquad (H \in \mathfrak{h}_1, f \in \mathcal{C}(\mathfrak{g}_0)).$$

Then T' is a $\mathcal{C}$-distribution on $\mathfrak{g}_0$ and we have to show that $T' = c$, where c is a constant. In Section 7, we shall obtain the weaker result that T' coincides with a constant on each connected component of the set of regular elements in $\mathfrak{g}_0$. The problem is thus reduced (see the corollary to Lemma 29) to proving that the various constants so obtained are all equal. This requires a deeper investigation which will be carried out in another paper.

In Section 8, we define the notion of a fundamental Cartan subalgebra and prove that any two such algebras are conjugate under G. Moreover, we show that

$$\lim_{H\to 0} \phi_f(H;\partial(\pi)) = 0 \qquad (H \in \mathfrak{h}_1, f \in \mathcal{C}(\mathfrak{g}_0))$$

if $\mathfrak{h}_0$ is not fundamental. Thus it only remains to study the case when $\mathfrak{h}_0$ is fundamental. In particular, this is so if $\mathfrak{h}_0 \subset \mathfrak{k}_0$, and so we again make this assumption. The principal result of Section 9 is contained in Theorem 4, and its proof is based on Theorem 5 of [2(h)]. The rest of this paper is devoted to proving that the constant c_0 of Theorem 4 is not zero. For this, we have to make use of some (unpublished) work of de Rham on the elementary solutions of a certain type of differential operators. (Similar results also appear to have been obtained by Gelfand and Graev [1].) We apply de Rham's formula to the operator $\partial(\omega)$, where ω is the Casimir polynomial of $\mathfrak{g}_0$. This enables us to prove (see Lemma 41) the existence of a connected component $\mathfrak{h}_1$ of $\mathfrak{h}_0'$ and of a function $g \in \mathcal{C}(\mathfrak{g}_0)$ such that

$$\lim_{H\to 0} \phi_g(H;\partial(\pi)) \neq 0 \qquad (H \in \mathfrak{h}_1).$$

We shall need this fact in our study of the general case when $\mathfrak{h}_0$ is fundamental but the corresponding Cartan subgroup is not necessarily compact.

The main results of Theorem 3 have been announced in a short note [2(i)] (see also [2(j)]).

2. A preliminary result. Let R and C be the fields of real and complex numbers, respectively, E_0 a vector space over R of finite dimension and F_0 a subspace of E_0. Let E be the complexification of E_0 and F the complexification of F_0 in E. We identify (real-valued) linear functions on E_0 with their linear extensions on E. Let E' be the space of all such functions. Then elements of E' will be called *real* linear functions on E. Let F' be the corresponding space for F. Then E' and F' are vector spaces over R. For any $\lambda \in E'$, let $\bar{\lambda}$ denote the restriction of λ on F. Then $\lambda \rightarrow \bar{\lambda}$ is a linear mapping of E' into F' whose kernel we denote by E_1'. Suppose we have introduced orders [2(f), §2] in E' and F'. Then these orders are said to be compatible if $\bar{\lambda} > 0$ implies $\lambda > 0$ $(\lambda \in E')$. Given any order in F', we can always define an order on E' compatible with it as follows. Select any order on E_1' and call an element $\lambda \in E'$ positive if either $\bar{\lambda}$ is positive in F', or $\lambda \in E_1'$ and it is positive in the order chosen in E_1'.

Let $\mathfrak{g}_0$ be a semisimple Lie algebra over R. Define $\mathfrak{k}_0$ and $\mathfrak{p}_0$ as in [2(c), §2] and let $\mathfrak{a}_{\mathfrak{p}_0}$ be a maximal abelian subspace of $\mathfrak{p}_0$. We extend it to a Cartan subalgebra $\mathfrak{a}_0$ of $\mathfrak{g}_0$. Then $\mathfrak{a}_0 = \mathfrak{a}_{\mathfrak{p}_0} + \mathfrak{a}_{\mathfrak{k}_0}$ where $\mathfrak{a}_{\mathfrak{k}_0} = \mathfrak{a}_0 \cap \mathfrak{k}_0$ (see [2(c), p. 188]). Complexify $\mathfrak{g}_0$ to $\mathfrak{g}$ and let $\mathfrak{k}$, $\mathfrak{p}$, $\mathfrak{a}_{\mathfrak{p}}$, $\mathfrak{a}$, $\mathfrak{a}_{\mathfrak{k}}$ denote the complexifications of $\mathfrak{k}_0$, $\mathfrak{p}_0$, $\mathfrak{a}_{\mathfrak{p}_0}$, $\mathfrak{a}_0$, $\mathfrak{a}_{\mathfrak{k}_0}$, respectively, in $\mathfrak{g}_0$. Now take[1] $E_0 = \mathfrak{a}_{\mathfrak{p}_0} + (-1)^{\frac{1}{2}}\mathfrak{a}_{\mathfrak{k}_0}$ and $F_0 = \mathfrak{a}_{\mathfrak{p}_0}$ in the above set up, and select compatible orders in the spaces of real linear functions on $\mathfrak{a}$ and $\mathfrak{a}_{\mathfrak{p}}$, respectively. Let $(\alpha_1, \cdots, \alpha_l)$ be a fundamental system [2(f), §2] of positive roots (of $\mathfrak{g}$ with respect to $\mathfrak{a}$) in our order. Then if $p = \dim \mathfrak{a}_{\mathfrak{p}} = \dim_R \mathfrak{a}_{\mathfrak{p}_0}$, we have the following result.

LEMMA 1. *It is possible to select p roots, say $(\alpha_1, \cdots, \alpha_p)$, among $(\alpha_1, \cdots, \alpha_l)$ with the following two properties.*[2]

(1) *$\bar{\alpha}_1, \cdots, \bar{\alpha}_p$ are linearly independent.*

(2) *If α is any root, $\bar{\alpha} = m_1\bar{\alpha}_1 + \cdots + m_p\bar{\alpha}_p$ where m_i are integers which are either all nonnegative or all nonpositive.*

Let Q be the set of all positive roots of $\mathfrak{g}$ in our order and Q_+ the subset consisting of those $\alpha \in Q$ for which $\bar{\alpha} \neq 0$. Select a minimal subset $(\alpha_1, \cdots, \alpha_q)$ (say) of our fundamental system such that, for every $\alpha \in Q_+$, $\bar{\alpha}$ can be written in the form $\bar{\alpha} = m_1\bar{\alpha}_1 + \cdots + m_q\bar{\alpha}_q$, where m_i are all nonnegative integers. Then it is enough to prove that $\bar{\alpha}_1, \cdots, \bar{\alpha}_q$ are linearly independent. This requires a few lemmas.

---

[1] We select once for all a square root of -1 in C and denote by $(-1)^{k/2}$ its k-th power for any integer k.

[2] The bar denotes restriction on $\mathfrak{a}_{\mathfrak{p}}$.

LEMMA 2. *If i, j are two distinct indices* $(1 \leqq i, j \leqq q)$, *then* $\bar{\alpha}_i - \bar{\alpha}_j \neq 0$ *or* $\bar{\alpha}$ *for any* $\alpha \in Q_+$.

Without loss of generality, we may assume that $i = 1$, $j = 2$. In view of the minimality of our system $(\alpha_1, \cdots, \alpha_q)$, it is obvious that $\bar{\alpha}_1 - \bar{\alpha}_2 \neq 0$. So let us now suppose that $\bar{\alpha}_1 = \bar{\alpha} + \bar{\alpha}_2$ for some $\alpha \in Q_+$. Then $\bar{\alpha}_1 = (m_1\bar{\alpha}_1 + \cdots + m_q\bar{\alpha}_q) + \bar{\alpha}_2$ where $m_1, \cdots, m_q$ are nonnegative integers. Hence

$$(m_1 - 1)\bar{\alpha}_1 + (m_2 + 1)\bar{\alpha}_2 + \sum_{3 \leqq k \leqq q} m_k\bar{\alpha}_k = 0.$$

It is clear that $m_1 = 0$, for otherwise, since $\bar{\alpha}_k > 0$ $(1 \leqq k \leqq q)$, the left side would be positive. Therefore

$$\bar{\alpha}_1 = (m_2 + 1)\bar{\alpha}_2 + \sum_{3 \leqq k \leqq q} m_k\bar{\alpha}_k,$$

and we get a contradiction with the minimality of the system $(\alpha_1, \cdots, \alpha_q)$.

Let B denote the fundamental bilinear form on $\mathfrak{g}$ [2(c), §2] and $\bar{\theta}$ the conjugation with respect to the compact real form $\mathfrak{u} = \mathfrak{k}_0 + (-1)^{\frac{1}{2}}\mathfrak{p}_0$. Then $\| X \|^2 = -B(X, \bar{\theta}(X))$ $(X \in \mathfrak{g})$ is a positive-definite Hermitian form on $\mathfrak{g}$. Since the restriction of B on $\mathfrak{a}_{\mathfrak{p}_0}$ is real and nondegenerate, for each real linear function λ on $\mathfrak{a}_{\mathfrak{p}}$, there exists a unique element $\Gamma_\lambda \in \mathfrak{a}_{\mathfrak{p}_0}$ such that $B(\Gamma, \Gamma_\lambda) = \lambda(\Gamma)$ for all $\Gamma \in \mathfrak{a}_{\mathfrak{p}}$. Define θ as in [2(c), §2].

LEMMA 3. *Suppose λ is a real linear function on $\mathfrak{a}_{\mathfrak{p}}$ and X an element in $\mathfrak{g}_0$ such that* $[\Gamma, X] = \lambda(\Gamma)X$ *for all* $\Gamma \in \mathfrak{a}_{\mathfrak{p}}$. *Then* $[\theta(X), X] = \| X \|^2 \Gamma_\lambda$.

Let $X = Y + Z$ $(Y \in \mathfrak{p}_0, Z \in \mathfrak{k}_0)$. Since $[\mathfrak{p}, \mathfrak{p}] \subset \mathfrak{k}$ and $[\mathfrak{p}, \mathfrak{k}] \subset \mathfrak{p}$, it follows that $[\Gamma, Y] = \lambda(\Gamma)Z$, $[\Gamma, Z] = \lambda(\Gamma)Y$ $(\Gamma \in \mathfrak{a}_{\mathfrak{p}})$. Moreover, $[\theta(X), X] = 2[Z, Y]$, and so it is clear that $[\theta(X), X]$ lies in $\mathfrak{p}_0$ and it commutes with every element in $\mathfrak{a}_{\mathfrak{p}_0}$. Therefore, since $\mathfrak{a}_{\mathfrak{p}_0}$ is maximal abelian in $\mathfrak{p}_0$, $[\theta(X), X] \in \mathfrak{a}_{\mathfrak{p}_0}$. Finally, if $\Gamma \in \mathfrak{a}_{\mathfrak{p}}$,

$$B(\Gamma, [\theta(X), X]) = -B([\Gamma, X], \theta(X)) = -\lambda(\Gamma)B(X, \theta(X)) = \lambda(\Gamma)\| X \|^2,$$

and this prove that $[\theta(X), X] = \| X \|^2 \Gamma_\lambda$.

For any two linear functions λ and μ on $\mathfrak{a}_{\mathfrak{p}}$, put $\langle \lambda, \mu \rangle = \lambda(\Gamma_\mu) = B(\Gamma_\lambda, \Gamma_\mu)$ and $| \lambda | = \langle \lambda, \lambda \rangle^{\frac{1}{2}} \geqq 0$. Then if $\lambda \neq 0$, $| \lambda | = \| \Gamma_\lambda \| > 0$. Let Σ be the set of all linear functions λ on $\mathfrak{a}_{\mathfrak{p}}$ for which there exists an element $X_\lambda \neq 0$ in $\mathfrak{g}_0$ with the property that $[\Gamma, X_\lambda] = \lambda(\Gamma)X_\lambda$ for all $\Gamma \in \mathfrak{a}_{\mathfrak{p}}$. It is obvious that Σ consists of zero and $\pm \bar{\alpha}$ $(\alpha \in Q_+)$.

LEMMA 4. *Suppose* $\lambda, \mu \in \Sigma$ *and* $\lambda - \mu \notin \Sigma$. *Then* $\langle \lambda, \mu \rangle \leqq 0$.

Select nonzero elements X_λ, X_μ in $\mathfrak{g}_0$ as above. We may assume that $\| X_\mu \| = 1$. It follows from our assumption that neither λ nor μ is zero. Put $X = 2^{\frac{1}{2}} | \mu |^{-1} X_\mu$, $Y = \theta(X)$ and $\Gamma_0 = 2 | \mu |^{-2} \Gamma_\mu$. Then $[Y, X] = \Gamma_0$, $[\Gamma_0, X] = 2X$, $[\Gamma_0, Y] = -2Y$. Hence $\mathfrak{l}_0 = RX + RY + R\Gamma_0$ is a three-dimensional Lie algebra and $Z \rightarrow \operatorname{ad} Z$ $(Z \in \mathfrak{l}_0)$ is a representation of $\mathfrak{l}_0$ on $\mathfrak{g}_0$. Now $(\operatorname{ad} \Gamma_0) X_\lambda = \lambda(\Gamma_0) X_\lambda$ and $(\operatorname{ad} Y) X_\lambda = 0$ since $\lambda - \mu \notin \Sigma$. Therefore it follows immediately from the theory of finite-dimensional representations of $\mathfrak{l}_0$ (see [2(a), Lemma 1]) that $\lambda(\Gamma_0) \leqq 0$. But $\lambda(\Gamma_0) = 2 | \mu |^{-2} \lambda(\Gamma_\mu)$, and so we conclude that $\langle \lambda, \mu \rangle \leqq 0$.

COROLLARY. *If* $i \neq j$ $(1 \leqq i, j \leqq q)$ *then* $\langle \bar{\alpha}_i, \bar{\alpha}_j \rangle \leqq 0$.

This is an immediate consequence of Lemmas 2 and 4.

Now we can prove that $\bar{\alpha}_1, \cdots, \bar{\alpha}_q$ are linearly independent. For otherwise, since they are real, we could select $a_i \in R$ $(1 \leqq i \leqq q)$ not all zero such that $a_1\bar{\alpha}_1 + \cdots + a_q\bar{\alpha}_q = 0$. We may suppose that $a_1, \cdots, a_k > 0$ while $a_{k+1}, \cdots, a_q \leqq 0$. Then if $b_j = -a_j$ $(k < j \leqq q)$,

$$a_1\bar{\alpha}_1 + \cdots + a_k\bar{\alpha}_k = b_{k+1}\bar{\alpha}_{k+1} + \cdots + b_q\bar{\alpha}_q = \lambda \quad \text{(say)}.$$

Therefore

$$| \lambda |^2 = \sum_{1 \leqq i \leqq k} \sum_{k < j \leqq q} a_i b_j \langle \bar{\alpha}_i, \bar{\alpha}_j \rangle \leqq 0$$

from the above corollary. This implies that $\lambda = a_1\bar{\alpha}_1 + \cdots + a_k\bar{\alpha}_k = 0$ which, however, is impossible since $\bar{\alpha}_1, \cdots, \bar{\alpha}_k$ are all positive and $a_1, \cdots, a_k > 0$. This completes the proof of Lemma 1.

3. Some inequalities. The positive-definite Hermitian form

$$\| X \|^2 = -B(X, \theta(X)) \qquad (X \in \mathfrak{g})$$

defines the structure of a Hilbert space on $\mathfrak{g}$. For any linear transformation T in $\mathfrak{g}$, put $\| T \|^2 = \operatorname{sp}(T^*T)$, where T^* is the adjoint of T with respect to this structure. It is clear that $(\operatorname{ad} X)^* = -\operatorname{ad}(\theta(X))$ $(X \in \mathfrak{g})$, and therefore $\| \operatorname{ad} X \| = \| X \|$. Let G be the connected adjoint group of $\mathfrak{g}_0$ and K the analytic subgroup of G corresponding to $\mathfrak{k}_0$. Then every element $k \in K$ is a unitary transformation on $\mathfrak{g}$, and therefore $\| k \| = 1$.

Let $\mathfrak{h}_0$ be a Cartan subalgebra of $\mathfrak{g}_0$. *Until the end of Section* 4 *we shall assume that* $\mathfrak{h}_0 \subset \mathfrak{k}_0$. Let $\mathfrak{h}$ denote the complexification of $\mathfrak{h}_0$ in $\mathfrak{g}$ and P the set of all positive roots (under some arbitrary but fixed order) of $\mathfrak{g}$ with respect to $\mathfrak{h}$. Let P_- and P_0 be the subsets of P consisting of the compact and the noncompact roots, respectively (see [2(f), p. 751]). Put $\pi_0 = \prod_{\alpha \in P_0} \alpha$. Then π_0 is a polynomial function on $\mathfrak{h}$.

LEMMA 5. *Suppose* $x \in G$ *and* $H \in \mathfrak{h}_0$. *Then*

$$\| xH + \theta(xH) \|^2 = 2 \| H \|^2 + 2 \| xH \|^2.$$

Moreover, there exist integers $m, q \geqq 0$ *and a positive number* c *such that*

$$\| x \| \, | \pi_0(H) |^q \leqq c \, \| xH + \theta(xH) \|^m$$

for all $x \in G$ *and* $H \in \mathfrak{h}_0$.

K being compact [5], any maximal abelian subalgebra of $\mathfrak{k}_0$ is conjugate to $\mathfrak{h}_0$ under K. Hence we can select $k \in K$ such that $k(\mathfrak{a}_{\mathfrak{k}_0}) \subset \mathfrak{h}_0$. Then $k(\mathfrak{a}_{\mathfrak{p}_0})$ is also a maximal abelian subspace of $\mathfrak{p}_0$, and therefore, by replacing $\mathfrak{a}_0$ by $k\mathfrak{a}_0$, we may assume that $\mathfrak{a}_{\mathfrak{k}_0} \subset \mathfrak{h}_c$. Let $A_{\mathfrak{p}}$ be the analytic subgroup of G corresponding to $\mathfrak{a}_{\mathfrak{p}_0}$. Then $G = KA_{\mathfrak{p}}K$ (see [2(g), §12]), and every element in K is a unitary transformation on $\mathfrak{g}$ which commutes with θ. Therefore for the proof of our lemma, it is obviously enough to consider the case when $x = ak$ $(a \in A_{\mathfrak{p}}, k \in K)$. Fix an element $H \in \mathfrak{h}_0$, and put $kH = X$. Then $xH = aX$ and $\theta(xH) = a^{-1}X$. Hence $\| xH + \theta(xH) \| = \| aX + a^{-1}X \|$. But since a is self-adjoint, it is obvious that $\| aX + a^{-1}X \|^2 = \| aX \|^2 + \| a^{-1}X \|^2 + 2 \| X \|^2$. Moreover, $\| a^{-1}X \| = \| \theta(aX) \| = \| aX \|$, and therefore

$$\| xH + \theta(xH) \|^2 = 2 \| X \|^2 + 2 \| aX \|^2 = 2 \| H \|^2 + 2 \| xH \|^2.$$

This proves the first assertion. The proof of the second statement is, however, more complicated.

Define Q and Q_+ as in Section 2, and for any root β of $\mathfrak{g}$ with respect to $\mathfrak{a}$, choose an element $X_\beta \neq 0$ in $\mathfrak{g}$ such that $[\Gamma, X_\beta] = \beta(\Gamma) X_\beta$ for all $\Gamma \in \mathfrak{a}$. Then the function $\theta\beta : \Gamma \rightarrow \beta(\theta\Gamma)$ is also a root.[3] Let Q_- be the complement of Q_+ in Q. Then if $\beta \in Q_-$, $\theta\beta = \beta$ and $X_\beta, X_{-\beta} \in \mathfrak{k}$. On the other hand $\theta\beta < 0$ if $\beta \in Q_+$. Put $\mathfrak{q} = \sum_{\beta \in Q_-} CX_\beta$, $\mathfrak{q}^- = \sum_{\beta \in Q_+} CX_{-\beta}$, and let $\mathfrak{l}$ be the centralizer of $\mathfrak{a}_{\mathfrak{p}}$ in $\mathfrak{k}$. Then $\mathfrak{l} \supset \mathfrak{a}_{\mathfrak{k}}$ and

$$\mathfrak{g} = \mathfrak{q}^- + \mathfrak{l} + \mathfrak{a}_{\mathfrak{p}} + \mathfrak{q} = \mathfrak{k} + \mathfrak{a}_{\mathfrak{p}} + \mathfrak{q} = \mathfrak{p} + \mathfrak{l} + \mathfrak{q},$$

where all the sums are direct.[3] Therefore

$$\dim \mathfrak{k} = \dim \mathfrak{g} - \dim \mathfrak{a}_{\mathfrak{p}} - \dim \mathfrak{q} = \dim \mathfrak{l} + \dim \mathfrak{q}.$$

Define a linear mapping ϕ of $\mathfrak{l} + \mathfrak{q}$ into $\mathfrak{k}$ by $\phi(X) = X + \theta(X)$ $(X \in \mathfrak{l} + \mathfrak{q})$. Since $(\mathfrak{l} + \mathfrak{q}) \cap \mathfrak{p} = \{0\}$, the kernel of ϕ is zero. Therefore since $\mathfrak{k}$ and $\mathfrak{l} + \mathfrak{q}$ have the same dimension, ϕ is an isomorphism of $\mathfrak{l} + \mathfrak{q}$ onto $\mathfrak{k}$.

---

[3] All the facts stated here are well known (see [2(c), p. 188]).

Now if $\Gamma \in \mathfrak{a}_{\mathfrak{p}_0}$, $\operatorname{ad}\Gamma$ is a self-adjoint operator on $\mathfrak{g}$, and its eigenvalues are zero and $\pm\beta(\Gamma)$ $(\beta \in Q_+)$. Therefore

$$\|(\operatorname{ad}\Gamma)^2 Z\| \geqq \lambda(\Gamma)\|(\operatorname{ad}\Gamma)Z\| \qquad (Z \in \mathfrak{g}, \Gamma \in \mathfrak{a}_{\mathfrak{p}_0}),$$

where $\lambda(\Gamma) = \min|\beta(\Gamma)|$ and β runs over all roots in Q_+ for which $\beta(\Gamma) \neq 0$. (In case $\Gamma = 0$, we put $\lambda(\Gamma) = 0$.)

Now select[4] $\alpha_1, \cdots, \alpha_p \in Q_+$ according to Lemma 1, and choose $\Gamma_i \in \mathfrak{a}_{\mathfrak{p}_0}$ $(1 \leqq i \leqq p)$ such that[5] $\alpha_i(\Gamma_j) = \delta_{ij}$ $(1 \leqq i, j \leqq p)$. Then $(\Gamma_1, \cdots, \Gamma_p)$ is a base for $\mathfrak{a}_{\mathfrak{p}_0}$ over R, and it is clear that $\lambda(\Gamma_i) \geqq |\alpha_i(\Gamma_i)| = 1$. Therefore

$$\|(\operatorname{ad}\Gamma_i)^2 Z\| \geqq \|(\operatorname{ad}\Gamma_i)Z\| \qquad (Z \in \mathfrak{g}, 1 \leqq i \leqq p).$$

Let Y be an element in $\mathfrak{q}_0 = \mathfrak{q} \cap \mathfrak{g}_0$. Then $\operatorname{ad} Y$ is nilpotent and $B(Y, Y) = B(\theta(Y), \theta(Y)) = 0$. Therefore

$$\|\phi(Y)\|^2 = -2B(Y, \theta(Y)) = 2\|Y\|^2.$$

Hence if $\mathfrak{l}_0 = \mathfrak{l} \cap \mathfrak{g}_0$ and $X \in \mathfrak{l}_0 + \mathfrak{q}_0$,

$$\|\phi((\operatorname{ad}\Gamma_i)^2 X)\|^2 = 2\|(\operatorname{ad}\Gamma_i)^2 X\|^2$$

since $(\operatorname{ad}\Gamma_i)^2 X \in \mathfrak{q}_0$. Moreover, $(\operatorname{ad}\Gamma_i)^2$ commutes with θ. Therefore

$$\|\phi((\operatorname{ad}\Gamma_i)^2 X)\| = \|(\operatorname{ad}\Gamma_i)^2\phi(X)\| \geqq \|(\operatorname{ad}\Gamma_i)\phi(X)\|$$

as we have seen above. Hence

$$\|(\operatorname{ad}\Gamma_i)^2 X\| \geqq 2^{-\frac{1}{2}}\|(\operatorname{ad}\Gamma_i)\phi(X)\| \qquad (X \in \mathfrak{l}_0 + \mathfrak{q}_0, 1 \leqq i \leqq p).$$

On the other hand, we know (see Iwasawa [3]) that $\mathfrak{g}_0$ is the direct sum of $\mathfrak{k}_0$, $\mathfrak{a}_{\mathfrak{p}_0}$ and $\mathfrak{q}_0$, so that

$$\begin{aligned}\dim_R \mathfrak{q}_0 &= \dim_R \mathfrak{g}_0 - \dim_R \mathfrak{k}_0 - \dim_R \mathfrak{a}_{\mathfrak{p}_0} \\ &= \dim \mathfrak{g} - \dim \mathfrak{k} - \dim \mathfrak{a}_{\mathfrak{p}} = \dim \mathfrak{q}.\end{aligned}$$

Therefore $\dim_R(\mathfrak{l}_0 + \mathfrak{q}_0) = \dim \mathfrak{l} + \dim \mathfrak{q} = \dim \mathfrak{k} = \dim_R \mathfrak{k}_0$. Since $\phi(\mathfrak{l}_0 + \mathfrak{q}_0)$ is obviously contained in $\mathfrak{g}_0$, it follows that ϕ defines a linear isomorphism of $\mathfrak{l}_0 + \mathfrak{q}_0$ onto $\mathfrak{k}_0$. Let ψ denote the inverse of this isomorphism. Then the above result may be written in the form

$$\|(\operatorname{ad}\Gamma_i)^2\psi(X)\| \geqq 2^{-\frac{1}{2}}\|(\operatorname{ad} X)\Gamma_i\| \qquad (X \in \mathfrak{k}_0, 1 \leqq i \leqq p).$$

Let $(\operatorname{ad} X)_{\mathfrak{p}}$ denote the restriction of $\operatorname{ad} X$ on $\mathfrak{p}$ $(X \in \mathfrak{k}_0)$, and put $\mu(X) = |\gamma|$, where γ is an eigenvalue of $(\operatorname{ad} X)_{\mathfrak{p}}$ with the smallest possible absolute value. Then since $\operatorname{ad} X$ is skew-adjoint, it is obvious that $\| (\operatorname{ad} X) Y \| \geqq \mu(X) \| Y \|$ $(Y \in \mathfrak{p})$. Therefore

---

[4] All our lemmas are true trivially when $\mathfrak{g}_0 = \mathfrak{k}_0$. So whenever it is convenient for the proof, we shall assume that $\mathfrak{p}_0 \neq \{0\}$.

[5] $\delta_{ij} = 1$ or 0 according as $i = j$ or $i \neq j$.

$$\prod_{i=1}^{p} \| (\operatorname{ad} \Gamma_i)^2 \psi(X) \| \geqq 2^{-p/2} \prod_{1 \leqq i \leqq p} \| (\operatorname{ad} X) \Gamma_i \| \geqq 2^{-p/2} \mu(X)^p \prod_{1 \leqq i \leqq p} \| \Gamma_i |.$$

Moreover it is obvious that $\mu(kX) = \mu(X)$ $(k \in K, X \in \mathfrak{k}_0)$. Hence

$$\prod_{1 \leqq i \leqq p} \| (\operatorname{ad} \Gamma_i)^2 \psi(kH) \| \geqq c_0 \mu(H)^p \qquad (H \in \mathfrak{h}_0, k \in K)$$

where $c_0 = 2^{-p/2} \prod_{1 \leqq i \leqq p} \| \Gamma_i \|$ is a positive constant. On the other hand, it follows from the definition of $\mu(H)$ that $\mu(H) = \min_{\beta \in P_0} | \beta(H) |$ $(H \in \mathfrak{h}_0)$. Therefore

$$\prod_{1 \leqq i \leqq p} \| (\operatorname{ad} \Gamma_i)^2 \psi(kH) \| \geqq c_0 \min_{\beta \in P_0} | \beta(H) |^p \qquad (H \in \mathfrak{h}_0, k \quad K).$$

Now observe that $| \beta(H) | \leqq \| H \|$ for any $\beta \in P$. Hence if q_0 is the number of roots in P_0,

$$\| H \|^{q_0 - 1} \min_{\beta \in P_0} | \beta(H) | \geqq \prod_{\beta \in P_0} | \beta(H) | = | \pi_0(H) |,$$

and therefore

$$\| H \|^{p(q_0 - 1)} \prod_{1 \leqq i \leqq p} \| (\operatorname{ad} \Gamma_i)^2 \psi(kH) \| \geqq c_0 | \pi_0(H) |^p \qquad (H \in \mathfrak{h}_0, k \in K).$$

Let $\mathfrak{a}_{\mathfrak{p}_0}^{+}$ be the set of all $\Gamma \in \mathfrak{a}_{\mathfrak{p}_0}$ such that $\alpha(\Gamma) \geqq 0$ for every $\alpha \in Q$. It is obvious that $\Gamma = t_1 \Gamma_1 + \cdots + t_p \Gamma_p$ $(t_i \in R)$ lies in $\mathfrak{a}_{\mathfrak{p}_0}^{+}$ if and only if $t_1, \cdots, t_p \geqq 0$. Let $A_{\mathfrak{p}}^{+}$ be the image of $\mathfrak{a}_{\mathfrak{p}_0}^{+}$ in $A_{\mathfrak{p}}$ under the exponential mapping. Then it is known (see [2(g), Lemma 38]) that $G = K A_{\mathfrak{p}}^{+} K$. Hence in the proof of the second assertion of our lemma, we can assume that $x \in A_{\mathfrak{p}}^{+} K$. Select a maximal set $(\alpha_1, \cdots, \alpha_r)$ $(r \geqq p)$ of roots in Q_+ such that $\bar{\alpha}_1, \cdots, \bar{\alpha}_r$ are all distinct. Then it is obvious that $\mathfrak{q} = \sum_{1 \leqq j \leqq r} \mathfrak{q}_j$, where $\mathfrak{q}_j$ is the set of all $Y \in \mathfrak{q}$ for which $[\Gamma, Y] = \alpha_j(\Gamma) Y (\Gamma \in \mathfrak{a}_{\mathfrak{p}})$. Moreover, $\operatorname{ad} \Gamma$ is self-adjoint for $\Gamma \in \mathfrak{a}_{\mathfrak{p}_0}$, and so it is clear that $\mathfrak{q}_j$ $(1 \leqq j \leqq r)$ are mutually orthogonal. Similarly $\mathfrak{l}$, $\mathfrak{q}$ and $\mathfrak{q}^-$ are orthogonal to each other. Now suppose $x = ak$ $(a \in A_{\mathfrak{p}}^{+}, k \in K)$ and H is a fixed element in $\mathfrak{h}_0$ such that $\pi_0(H) \neq 0$. Then if $\psi(kH) = L + X$ $(L \in \mathfrak{l}_0, X \in \mathfrak{q}_0)$, we have $kH = 2L + X + \theta(X)$. Hence

$$\begin{aligned} \| xH + \theta(xH) \|^2 &= 2 \| H \|^2 + 2 \| xH \|^2 \\ &= 16 \| L \|^2 + 4 \| X \|^2 + 2 \| aX \|^2 + 2 \| a^{-1} X \|^2. \end{aligned}$$

Put $\nu = \max_{\alpha, i} | \alpha(\Gamma_i) |$ for $\alpha \in Q$ and $1 \leqq i \leqq p$. Then since no eigenvalue of

$\operatorname{ad}\Gamma_i$ can exceed ν in absolute value, $\|(\operatorname{ad}\Gamma_i)^2 Z\| \leqq \nu^2 \|Z\|$ $(Z \in \mathfrak{g}, 1 \leqq i \leqq p)$. Therefore if $a = \exp\Gamma$ $(\Gamma \in \mathfrak{a}_{\mathfrak{p}_0}{}^+)$ and X_j is the orthogonal projection of X in $\mathfrak{q}_j$, we have

$$\|aX\|^2 \geqq \nu^{-4}\|(\operatorname{ad}\Gamma_i)^2 aX\|^2 = \nu^{-4}\sum_{1\leqq j\leqq r} e^{2\alpha_j(\Gamma)}\alpha_j(\Gamma_i)^4\|X_j\|^2 \qquad (1 \leqq i \leqq p).$$

Now we claim that

$$e^{\alpha(\Gamma)}\alpha(\Gamma_i)^2 \geqq e^{\alpha_i(\Gamma)}\alpha(\Gamma_i)^2$$

for $\alpha \in Q_+$. This is obvious if $\alpha(\Gamma_i) = 0$, and so let us suppose that $\alpha(\Gamma_i) \neq 0$. We know that $\bar\alpha = \nu_1\bar\alpha_1 + \cdots + \nu_p\bar\alpha_p$, where $\nu_j = \alpha(\Gamma_j)$ $(1 \leqq j \leqq p)$ are nonnegative integers. Therefore, since $\Gamma \in \mathfrak{a}_{\mathfrak{p}_0}{}^+$ and $\nu_i = \alpha(\Gamma_i) \geqq 1$, we conclude that $\alpha(\Gamma) \geqq \nu_i\alpha_i(\Gamma) \geqq \alpha_i(\Gamma)$, and our inequality follows. This shows that $\|aX\|^2 \geqq \nu^{-4}\sum_{1\leqq j\leqq r} e^{2\alpha_i(\Gamma)}\alpha_j(\Gamma_i)^4\|X_j\|^2 = \nu^{-4}e^{2\alpha_i(\Gamma)}\|(\operatorname{ad}\Gamma_i)^2X\|^2$ $(1 \leqq i \leqq p)$, and therefore

$$\|xH + \theta(xH)\|^p \geqq \|aX\|^p \geqq \nu^{-2p}e^{\gamma(\Gamma)}\prod_{1\leqq i\leqq p}\|(\operatorname{ad}\Gamma_i)^2X\|,$$

where $\gamma = \alpha_1 + \alpha_2 + \cdots + \alpha_p$. On the other hand,

$$\|x\|^2 = \|a\|^2 = \operatorname{sp} a^2 = l + \sum_{\alpha\in Q}(e^{2\alpha(\Gamma)} + e^{-2\alpha(\Gamma)}),$$

where $l = \dim\mathfrak{a}$. Moreover, it is obvious that $\alpha(\Gamma) \leqq \nu\gamma(\Gamma)$ for any $\alpha \in Q$. Therefore if $n = \dim\mathfrak{g}$, $\|x\|^2 \leqq ne^{2\nu\gamma(\Gamma)}$. Also $(\operatorname{ad}\Gamma_i)^2\psi(kH) = (\operatorname{ad}\Gamma_i)^2X$. Hence it follows from our earlier result and the first assertion of the lemma that

$$\begin{aligned}\|x\| &\leqq n^{\frac12}\nu^{2p\nu}\|xH + \theta(xH)\|^{p\nu}\{\prod_{1\leqq i\leqq p}\|(\operatorname{ad}\Gamma_i)^2X\|\}^{-\nu}\\ &\leqq n^{\frac12}\nu^{2p\nu}\|xH + \theta(xH)\|^{p\nu}\{c_0|\pi_0(H)|^p\|H\|^{-p(q_0-1)}\}^{-\nu}\\ &\leqq n^{\frac12}\nu^{2p\nu}\|xH + \theta(xH)\|^{p\nu}\{c_0|\pi_0(H)|^p\|xH + \theta(xH)\|^{-p(q_0-1)}\}^{-\nu}.\end{aligned}$$

So by taking $q = p\nu$, $m = p\nu q_0$ and $c = n^{\frac12}\nu^{2p\nu}c_0{}^{-\nu}$, we get the second statement of the lemma.

LEMMA 6. *Let λ be any real linear function on $\mathfrak{a}_{\mathfrak{p}}$. Then there exists an integer $m \geqq 0$ such that*

$$e^{\lambda(\Gamma)} \leqq \|\exp\Gamma\|^m$$

for $\Gamma \in \mathfrak{a}_{\mathfrak{p}_0}{}^+$.

It is clear that[4]

$$\|\exp\Gamma\|^2 \geqq \sum_{\alpha\in Q_+} e^{2\alpha(\Gamma)} \geqq r\exp(2r^{-1}\sum_{\alpha\in Q_+}\alpha(\Gamma)) \qquad (\Gamma \in \mathfrak{a}_{\mathfrak{p}_0}{}^+),$$

where r is the number of roots in Q_+. Moreover, we can obviously choose a positive integer s such that

$$s(\alpha_1(\Gamma)+\alpha_2(\Gamma)+\cdots+\alpha_p(\Gamma))\geqq\lambda(\Gamma)$$

for $\Gamma\in\mathfrak{a}_{\mathfrak{p}_0}{}^+$. Therefore

$$\|\exp\Gamma\|^{rs}\geqq\exp(s\sum_{\alpha\in Q_+}\alpha(\Gamma))\geqq\exp\lambda(\Gamma)\qquad(\Gamma\in\mathfrak{a}_{\mathfrak{p}_0}{}^+),$$

and this proves the lemma.

COROLLARY 1. *Let dx denote the Haar measure of G. Then there exists an integer $s\geqq 0$ such that*

$$\int_G\|x\|^{-s}\,dx<\infty.$$

Let dk and $d\Gamma$, respectively, denote the Haar measure on K and the Euclidean measure on $\mathfrak{a}_{\mathfrak{p}_0}$. Then it is known (see [2(g), Lemma 38]) that one can normalize dx in such a way that

$$\int_G g(x)\,dx=\int_{K\times\mathfrak{a}_{\mathfrak{p}_0}{}^+\times K}g(k(\exp\Gamma)k')\mu(\Gamma)\,dk\,d\Gamma\,dk'\qquad(g\in C_c(G)).$$

Here $C_c(G)$ is the set of all continuous functions on G which vanish outside a compact set and

$$\mu(\Gamma)=\prod_{\alpha\in Q_+}(e^{\alpha(\Gamma)}-e^{-\alpha(\Gamma)}).$$

It is obvious that

$$\mu(\Gamma)\leqq\exp(\sum_{\alpha\in Q_+}\alpha(\Gamma))\qquad(\Gamma\in\mathfrak{a}_{\mathfrak{p}_0}{}^+).$$

Select a real linar function λ on $\mathfrak{a}_\mathfrak{p}$ such that $\int_{\mathfrak{a}_{\mathfrak{p}_0}{}^+}e^{-\lambda(\Gamma)}\,d\Gamma<\infty$. Then from Lemma 6,

$$\exp(\lambda(\Gamma)+\sum_{\alpha\in Q_+}\alpha(\Gamma))\leqq\|\exp\Gamma\|^s\qquad(\Gamma\in\mathfrak{a}_{\mathfrak{p}_0}{}^+)$$

for some integer s. Hence

$$\mu(\Gamma)\|\exp\Gamma\|^{-s}\leqq e^{-\lambda(\Gamma)},$$

and therefore

$$\int_G\|x\|^{-s}\,dx=\int_{\mathfrak{a}_{\mathfrak{p}_0}{}^+}\|\exp\Gamma\|^{-s}\mu(\Gamma)\,d\Gamma\leqq\int_{\mathfrak{a}_{\mathfrak{p}_0}{}^+}e^{-\lambda(\Gamma)}\,d\Gamma<\infty$$

if we assume that $\int_K dk=1$.

Let σ be a representation of G on a finite-dimensional Hilbert space V.

For any linear transformation T on V, put $\| T \| = \{\mathrm{sp}(T^*T)\}^{\frac{1}{2}}$, where T^* is the adjoint of T.

COROLLARY 2. *We can find an integer* $m \geqq 0$ *and a positive number* c *such that* $\| \sigma(x) \| \leqq c \| x \|^m$ *for all* $x \in G$.

Let us denote the corresponding representation of $\mathfrak{g}$ also by σ. If S is a nonsingular linear transformation on V, we know that $\| S\sigma(x)S^{-1} \| \leqq \| S \| \| \sigma(x) \| \| S^{-1} \|$, and therefore it is permissible, for our proof, to replace σ by an equivalent representation on V. Since $\mathfrak{u} = \mathfrak{k}_0 + (-1)^{\frac{1}{2}}\mathfrak{p}_0$ is a compact real form of $\mathfrak{g}$, we may, by going over to an equivalent representation, assume that $\sigma(X)$ is skew-adjoint for $X \in \mathfrak{u}$. Then $\sigma(k)$ is unitary and $\sigma(a)$ self-adjoint ($k \in K, a \in A_{\mathfrak{p}}$). Therefore, since $G = KA_{\mathfrak{p}}{}^+K$, it is enough to consider the case when $x \in A_{\mathfrak{p}}{}^+$. Let $d = \dim V$ and $\Lambda_1, \cdots, \Lambda_r$ be all the distinct weight of σ (with respect to $\mathfrak{a}$). Then Λ_i are all real linear functions on $\mathfrak{a}$ and so from Lemma 6, we can choose an integer $m \geqq 0$ such that $e^{\Lambda_i(\Gamma)} \leqq \| \exp \Gamma \|^m$ $(1 \leqq i \leqq r)$ for $\Gamma \in \mathfrak{a}_{\mathfrak{p}_0}{}^+$. This proves that

$$\| \sigma(a) \|^2 \leqq d \max_i e^{2\Lambda_i(\Gamma)} \leqq d \| a \|^{2m}$$

if $a = \exp \Gamma$ $(\Gamma \in \mathfrak{a}_{\mathfrak{p}_0}{}^+)$.

4. Applications of the above inequalities. Let $\mathcal{S}_0$ denote the set of all continuous functions f on $\mathfrak{g}_0$ such that

$$\nu_m(f) = \sup_{X \in \mathfrak{g}_0} | f(X) | (1 + \| X + \theta(X) \|)^m < \infty$$

for every integer $m \geqq 0$. Also let $\mathfrak{h}_0{}''$ denote the set of those points $H \in \mathfrak{h}_0$ where $\pi_0(H) \neq 0$.

LEMMA 7. *Let m be a given integer* $\geqq 0$. *Then we can find integers* $q, m_1 \geqq 0$ *and a positive number* c, *such that*

$$(1 + \| H \|)^{q_1} | \pi_0(H) |^q \int_G \| x \|^m | f(xH) | \, dx \leqq c\nu_{m_1+q_1}(f)$$

for $H \in \mathfrak{h}_0{}''$, $f \in \mathcal{S}_0$ *and any integer* $q_1 \geqq 0$. *Moreover if* Ω *is a compact subset of* $G \times \mathfrak{h}_0{}'' \times G$ *and* $f \in \mathcal{S}_0$, *the integral*

$$\int_G \| zxy \|^m | f(zxyH) | \, dx$$

converges uniformly with respect to $(z, H, y) \in \Omega$.

Choose an integer $s \geqq 0$ such that $\int_G \| x \|^{-s} dx < \infty$ (Corollary 1 to

Lemma 6). Then from Lemma 5, we can select integers $q, m_1 \geqq 0$ and a positive number c_1 with the property that

$$|\pi_0(H)|^q \| x \|^{m+s} \leqq c_1 \| xH + \theta(xH) \|^{m_1}$$

for all $H \in \mathfrak{h}_0$ and $x \in G$. Then since $\| H \| \leqq \| xH + \theta(xH) \|$ (Lemma 5),

$$(1 + \| H |)^{q_1} | \pi_0(H) |^q \| x \|^m | f(xH) | \leqq c_1 \nu_{m_1+q_1}(f) \| x \|^{-s},$$

and therefore if we put

$$c = c_1 \int \| x \|^{-s} \, dx,$$

our first assertion follows. Now suppose $(z, H, y) \in \Omega$ and $f \in \mathscr{S}_0$. Then

$$\| zxy \|^m | f(zxyH) \leqq c_1 | \pi_0(H) |^{-q} \nu_{m_1}(f) \| zxy \|^{-s}.$$

But $\| x \| = \| z^{-1}(zxy) y^{-1} \| \leqq \| z^{-1} \| \| zxy \| \| y^{-1} \|$. Therefore

$$\| zxy \| \geqq \| z^{-1} \|^{-1} \| x \| \| y^{-1} \|^{-1}$$

and

$$\| zxy \|^m | f(zxyH) | \leqq c_1 | \pi_0(H) |^{-q} \nu_{m_1}(f) \| z^{-1} \|^s \| y^{-1} \|^s \| x \|^{-s}$$

It is obvious that $| \pi_0(H) |^{-q} \| z^{-1} \|^s \| y^{-1} |^s$ remains bounded on the compact set Ω, and so our statement about uniform convergence follows from the fact that $\int \| x \|^{-s} \, dx < \infty$.

From now on we shall make use of the notation and terminology of [2(h)] without further comment. Let $\mathscr{S}$ be the set of all $f \in C^\infty(\mathfrak{g}_0)$ such that $Df \in \mathscr{S}_0$ for every $D \in \partial(S(\mathfrak{g}))$. Let $\mathfrak{B}$ be the universal enveloping algebra of $\mathfrak{g}$, and define Γ_X $(X \in \mathfrak{g}_0)$ as in [2(h), §3]. Then we have seen (Lemma 3 of [2(h)]) that

$$g(x; b : X; \partial(\xi)) = g(x : X; \partial(\Gamma_X(b \mathbf{X} \xi))),$$

where $g \in C^\infty(\mathfrak{g}_0)$, $b \in \mathfrak{B}$, $\xi \in S(\mathfrak{g})$, $x \in G$ and $X \in \mathfrak{g}_0$. Suppose b and ξ are fixed. Then it is clear, from the definition of Γ_X, that we can select a finite number of linearly independent elements $\xi_1, \cdots, \xi_r \in S(\mathfrak{g})$ and also $p_1, \cdots, p_r \in S(\mathfrak{g})$ such that

$$\Gamma_X(b \mathbf{X} \xi) = p_1(X)\xi_1 + \cdots + p_r(X)\xi_r \qquad (X \in \mathfrak{g}_0).$$

Therefore

$$g(x; b : X; \partial(\xi)) = \sum_{1 \leqq i \leqq r} p_i(X) g(x : X; \partial(\xi_i)).$$

On the other hand, if $\eta \in S(\mathfrak{z})$,

$$g(x : X; \partial(\eta)) = g(xX; \partial(\eta^x)).$$

Therefore

$$g(x:X;\partial(\xi_i))=g(xX;\partial(\xi_i^x)) \qquad (1\leqq i\leqq r),$$

and again we can select a finite number of linearly independent elements η_j $(1\leqq j\leqq s)$ in $S(\mathfrak{g})$ such that

$$\xi_i^x=\sum_{1\leqq j\leqq s}a_{ij}(x)\eta_j \qquad (1\leqq i\leqq r),$$

where a_{ij} are analytic functions on G. Moreover, we know from Corollary 2 to Lemma 6 that $|a_{ij}(x)|\leqq a\|x\|^m$ $(x\in G)$, where m is a suitable non-negative integer and a a positive constant. Then

$$|g(x;b:X;\partial(\xi))|\leqq a\|x\|^m\sum_{i,j}|p_i(X)||g(xX;\partial(\eta_j))|.$$

Now suppose $g\in\mathcal{S}$. Then $\partial(\eta_j)g\in\mathcal{S}_0$, and it follows from Lemma 7, that

$$\int\|xy\|^m|g(xyH;\partial(\eta_j)|\,dx$$

converges uniformly with respect to (y,H) on every compact subset Ω of $G\times\mathfrak{h}_0''$. Thus we have obtained the following result.

LEMMA 8. *Suppose $f\in\mathcal{S}$, $b\in\mathfrak{B}$ and $\xi\in S(\mathfrak{g})$. Then if Ω is a compact subset of $G\times\mathfrak{h}_0''$, the integral*

$$\int_G|f(xy;b:H;\partial(\xi))|\,dx$$

converges uniformly with respect to $(y,H)\in\Omega$.

Put $\mathfrak{B}'=\mathfrak{B}\mathfrak{g}$.

COROLLARY 1. *The notation being as above,*

$$\int_G f(x;b:H;\partial(\xi))\,dx=0$$

if $b\in\mathfrak{B}'$.

For a fixed $H\in\mathfrak{h}_0''$, put

$$F(y)=\int_G f(xy:H;\partial(\xi))\,dx \qquad (y\in G).$$

Then it follows from Lemma 8 that F is of class C^∞ on G and

$$F(y;b)=\int_G f(xy;b:H;\partial(\xi))\,dx$$

for $b\in\mathfrak{B}$. But since the above integral for $F(y)$ converges absolutely, it follows from the right invariance of the Haar measure of G, that $F(y)$ is actually independent of y. Therefore $F(y;b)=0$ if $b\in\mathfrak{B}'$, and our assertion follows by putting $y=1$.

COROLLARY 2. *Put* $\phi_f'(H)=\int_G f(xH)\,dx$ *for* $f\in\mathcal{S}$ *and* $H\in\mathfrak{h}_0''$. *Then* ϕ_f' *is of class* C^∞ *on* $\mathfrak{h}_0''$ *and if* $v\in S(\mathfrak{h})$,

$$\phi_f'(H;\partial(v))=\int_G f(x:H;\partial(v))\,dx \qquad (H\in\mathfrak{h}_0'').$$

This is an immediate consequence of the uniform convergence of

$$\int_G |f(x:H;\partial(v))|\,dx \qquad (v\in S(\mathfrak{h}))$$

with respect to H on each compact subset of $\mathfrak{h}_0''$.

LEMMA 9. *For given* $b\in\mathfrak{B}$ *and* $\xi\in S(\mathfrak{g})$, *we can select integers* $q, M\geqq 0$ *and a finite number of elements* $d_1,\cdots,d_r\in\partial(S(\mathfrak{g}))$ *such that*

$$|\pi_0(H)|^q(1+\|H\|)^{q_1}\int |f(x;b:H;\partial(\xi))|\,dx\leqq\sum_{1\leqq i\leqq r}\nu_{M+q_1}(d_if) \qquad (H\in\mathfrak{h}_0'')$$

for $f\in\mathcal{S}$ *and any integer* $q_1\geqq 0$.

Let us keep to the notation of the proof of Lemma 8. Select q, m_1 and c corresponding to Lemma 7. Since p_i are polynomials, we can select an integer $q_2\geqq 0$ and a positive number c_1 such that

$$|p_i(X)|\leqq c_1(1+\|X\|)^{q_2} \qquad (1\leqq i\leqq r)$$

for all $X\in\mathfrak{g}$. Then if $q_1\geqq 0$, $f\in\mathcal{S}$ and $H\in\mathfrak{h}_0''$,

$$\begin{aligned}(1+\|H\|)^{q_1}|\pi_0(H)|^q&\int |f(x;b:H;\partial(\xi))|\,dx\\ &\leqq|\pi_0(H)|^q(1+\|H\|)^{q_1+q_2}ac_1r\sum_j\int\|x\|^m|f(xH;\partial(\eta_j))|\,dx\\ &\leqq acc_1r\sum_j\nu_{m_1+q_1+q_2}(\partial(\eta_j)f).\end{aligned}$$

The assertion of the lemma is now obvious.

Define ϕ_f' $(f\in\mathcal{S})$ as in Corollary 2 to Lemma 8.

COROLLARY. *For each* $d\in\mathfrak{D}(\mathfrak{h})$, *there exist integers* $q, m\geqq 0$ *and a finite number of elements* $d_1,\cdots,d_r\in\partial(S(\mathfrak{g}))$ *such that*

$$|\pi_0(H)|^q(1+\|H\|)^{q_1}|\phi_f'(H;d)|\leqq\sum_{1\leqq i\leqq r}\nu_{m+q_1}(d_if) \qquad (H\in\mathfrak{h}_0'')$$

for $f\in\mathcal{S}$ *and any integer* $q_1\geqq 0$.

It is obviously enough to prove this when d is of the form $u\partial(v)$ $(u, v \in S(\mathfrak{g}))$. Select an integer $q_2 \geqq 0$ and a positive number c such that $|u(H)| \leqq c(1 + \| H \|)^{q_2}$ $(H \in \mathfrak{h})$. Then

$$|\phi_f'(H;d)| \leqq c(1 + \| H \|)^{q_2} \int |f(x:H;\partial(v))|\,dx$$

from Corollary 2 to Lemma 8, and the desired result now follows from Lemma 9.

We recall that $I(\mathfrak{g})$ is the algebra of those polynomials in $S(\mathfrak{g})$ which are invariant under G, and for any $p \in S(\mathfrak{g})$, $\bar{p}$ denotes the restriction of p on $\mathfrak{h}$. Furthermore, $\pi = \prod_{\alpha \in P} \alpha$.

THEOREM 1. *For any* $f \in \mathcal{S}$, *put*

$$\phi_f(H) = \pi(H) \int_G f(xH)\,dx \qquad (H \in \mathfrak{h}_0'').$$

Then ϕ_f *is a function of class* C^∞ *on* $\mathfrak{h}_0''$ *and*

$$\phi_{\partial(\xi)f} = \partial(\bar{\xi})\phi_f \qquad (\xi \in I(\mathfrak{g})).$$

The first statement follows from Corollary 2 to Lemma 8. Let $\mathfrak{h}_0'$ be the set of those points $H \in \mathfrak{h}_0$ where $\pi(H) \neq 0$. Then $\mathfrak{h}_0'$ is a dense subset of $\mathfrak{h}_0''$, and so for a fixed $\xi \in I(\mathfrak{g})$, it would be enough to prove that $\phi_{\partial(\xi)f} - \partial(\bar{\xi})\phi_f$ is zero on $\mathfrak{h}_0'$. Fix an element $H \in \mathfrak{h}_0'$, and put $d = \partial(\bar{\xi}) \circ \pi$. Then $d \in \mathfrak{D}(\mathfrak{h})$, and we know from Lemma 8 of [2(h)] that

$$f(xH;\partial(\xi)) = \pi(H)^{-1} f(x:H;d_H) + \sum_{1 \leqq i \leqq r} f(x;b_i:H;\partial(v_i)) \qquad (x \in G),$$

where $b_i \in \mathfrak{B}'$, $v_i \in S(\mathfrak{h})$ $(1 \leqq i \leqq r)$ and d_H is the local expression of d at H. Therefore it follows from Lemma 8 and its corollaries that

$$\begin{aligned}\phi_{\partial(\xi)f}(H) &= \pi(H) \int f(xH;\partial(\xi))\,dx = \int f(x:H;d_H)\,dx \\ &= \phi_f'(H;d) = \phi_f(H;\partial(\bar{\xi})).\end{aligned}$$

This proves the theorem.

For any integer $m \geqq 0$ and $d \in \partial(S(\mathfrak{g}))$, consider the function $\nu_{m,d}$: $f \to \nu_m(df)$ $(f \in \mathcal{S})$ on $\mathcal{S}$. Obviously, it is a seminorm, and we can define a topology on $\mathcal{S}$ by means of the collection of all such seminorms $\nu_{m,d}$. In this way $\mathcal{S}$ becomes a locally convex space. Since $\mathfrak{h}_0''$ is an open subset of $\mathfrak{h}_0$, the space $\mathcal{E}(\mathfrak{h}_0'')$ can be defined as usual (see [2(h), §2]).

THEOREM 2. *For any* f *in* $\mathcal{S}$, ϕ_f *lies in* $\mathcal{E}(\mathfrak{h}_0'')$ *and* $f \to \phi_f$ *is a continuous mapping of* $\mathcal{S}$ *into* $\mathcal{E}(\mathfrak{h}_0'')$.

Let U be a subset of $\mathfrak{h}_0''$. We shall say that U has property (A) if for every $v \in S(\mathfrak{h})$, we can select an integer $M \geqq 0$, a real constant $c \geqq 1$ and a finite number of elements $d_1, \cdots, d_r \in \partial(S(\mathfrak{g}))$ such that

$$(1 + \| H \|)^{q'} | \phi_f(H; \partial(v)) | \leqq c^{q'} \sum_{1 \leqq j \leqq r} \nu_{M+q'}(d_j f) \tag{A}$$

for $H \in U$, $f \in \mathscr{S}$ and all integers $q' \geqq 0$. Clearly the union of a finite number of sets with property (A) again has the same property. Similarly (A) holds for the closure of U in $\mathfrak{h}_0''$ whenever it holds for U. Let w be the order of the Weyl group W (of $\mathfrak{g}$ with respect to $\mathfrak{h}$). From Lemma 11 of [2(h)], we can select homogeneous elements $v_1, \cdots, v_w \in S(\mathfrak{h})$, such that $S(\mathfrak{h}) = \sum_{1 \leqq i \leqq w} I(\mathfrak{h}) v_i$. For any $v \in S(\mathfrak{h})$, let $\gamma_i(v)$ denote the unique elements in $I(\mathfrak{g})$ such that $v = \sum_{1 \leqq i \leqq w} \overline{\gamma_i(v)} v_i$ (see [2(h), Lemmas 9 and 11]), and put $D_i(v) = \partial(\gamma_i(v))$. Then if $f \in \mathscr{S}$, we know from Theorem 1 that

$$\partial(v) \phi_f = \sum_{1 \leqq i \leqq w} \partial(v_i) \phi_{D_i(v)f},$$

and therefore

$$| \phi_f(H; \partial(v)) | \leqq \sum_{1 \leqq i \leqq w} | \phi_{D_i(v)f}(H; \partial(v_i)) | \qquad (H \in \mathfrak{h}_0'').$$

This shows that in order to prove that U has property (A), it is enough to check this property for $v = v_1, v_2, \cdots, v_w$ only. Finally, it is obvious that Theorem 2 would be proved if we can show that $\mathfrak{h}_0''$ has property (A).

Since $\mathfrak{h}_0'$ is a dense subset of $\mathfrak{h}_0''$ and it has only a finite number of connected components, it is enough to prove that each connected component of $\mathfrak{h}_0'$ has property (A). Let $\mathfrak{h}_+$ be a connected component of $\mathfrak{h}_0'$ and P' the set of those roots α (of $\mathfrak{g}$ with respect to $\mathfrak{h}$) for which $-(-1)^{\frac{1}{2}}\alpha$ takes only positive values on $\mathfrak{h}_+$. Then we can select a fundamental system $(\alpha_1, \cdots, \alpha_l)$ of roots in P' (see [2(f), p. 749]). Choose a base $H_1, \cdots, H_l$ for $\mathfrak{h}_0$ over R such that $\alpha_i(H_j) = (-1)^{\frac{1}{2}} \delta_{ij}$ $(1 \leqq i, j \leqq l)$, and let $(t_1, \cdots, t_l)$ denote the system of Cartesian coordinates in $\mathfrak{h}_0$ corresponding to this base. By a monomial we shall mean a function T on $\mathfrak{h}_0$ of the form $T = t_1^{q_1} t_2^{q_2} \cdots t_l^{q_l}$, where $q_1, \cdots, q_l$ are nonnegative integers. q_i is called the exponent of t_i in T. In particular the monomial whose exponents are all zero is 1. We introduce a lexicographic order in the set of all monomials as follows. Suppose $T = t_1^{q_1} \cdots t_l^{q_l}$, $T' = t_1^{q_1'} \cdots t_l^{q_l'}$ are two distinct monomials. Then we say that $T \prec T'$ (or $T' \succ T$) if $q_i < q_i'$ where i is the least index $(1 \leqq i \leqq l)$ such that $q_i \neq q_i'$. It is obvious that every nonempty set of monomials has a lowest element. Furthermore, observe that every monomial takes only positive values on $\mathfrak{h}_+$. We say that a monomial T has property on τ_-. Put $c_2 = cc_1^2$, $r' = r(w^2+1)$, and let d_j' $(1 \leqq j \leqq r')$ denote the r' differential operators $d_j\partial(p_{hk})$ and d_j $(1 \leqq j \leqq r, 1 \leqq h, k \leqq w)$. Then since f and q' were arbitrary, the above result shows that

$$T_1\mu^{q'} \mid \partial(v_i)\phi_g \mid \leqq c_2^{q'}\{ \sum_{1 \leqq j \leqq r'} \nu_{M+q'}(d_j'g)\}(1 + \mid \log t \mid)$$

on τ_- for any $g \in \mathcal{S}$ and $q' \geqq 0$. Applying this result to $\partial(p_{hk})f$, we obtain

$$\mu^{q'} \mid \psi_i \mid \leqq c_2^{q'}a'_{q'}(1 + \mid \log t \mid) \qquad (1 \leqq i \leqq w, q' \geqq 0)$$

on τ_-, where

$$a'_{q'} = \sum_{1 \leqq j \leqq r'} \sum_{1 \leqq h,k \leqq w} \nu_{M+q'}(d_j'\partial(p_{hk})f).$$

Again, we find by integration that if $H \in \tau_-$,

$$\begin{aligned} \mid \phi_i(H) \mid &\leqq \mid \phi_i(H_0) \mid + \int_{t(H)}^{1} \mid \psi_i(H_0 - (1-s)H_m) \mid ds \\ &\leqq \{c^{q'}b_{q'} + 2(c_1c_2)^{q'}a'_{q'}\}(\bar{\mu}(H))^{-q'}, \end{aligned}$$

since $\int_0^1 (1 + \mid \log s \mid)\,ds = 2$. Therefore

$$\mu^{q'} \mid \phi_i \mid \leqq c_3^{q'}(b_{q'} + a'_{q'})$$

on τ_-, where $c_3 = 2c_1^2c_2$. On the other hand, since $q = 1$,

$$\mu^{q'} \mid \phi_i \mid \leqq t\mu^{q'} \mid \phi_i \mid \leqq c^{q'}b_{q'} \leqq c_3^{q'}b_{q'}$$

on τ_+. Therefore

$$\mu^{q'}T_1 \mid \partial(v_i)\phi_f \mid \leqq c_3^{q'}\{ \sum_{1 \leqq j \leqq r'} \sum_{1 \leqq h,k \leqq w} \nu_{M+q'}(d_j'\partial(p_{hk})f) + \sum_{1 \leqq j \leqq r} \nu_{M+q'}(d_jf)\}$$

on $\mathfrak{h}_+$ for $q' \geqq 0$ and $1 \leqq i \leqq w$. Again, since f is an arbitrary element of $\mathcal{S}$ and c_3 is independent of f and q', it is clear that the monomial T_1 has property (A′), and so we get a contradiction as before. This completes the proof of Theorem 2.

5. The general case. We shall now discard the assumption that $\mathfrak{h}_0 \subset \mathfrak{k}_0$ and try to extend Theorems 1 and 2 of Section 4 to the general case. But first we need some preliminary work.

As before let $\bar{\theta}$ denote the conjugation of $\mathfrak{g}$ with respect to its compact real form $\mathfrak{u} = \mathfrak{k}_0 + (-1)^{\frac{1}{2}}\mathfrak{p}_0$.

LEMMA 10. *Let* $\mathfrak{m}$ *be a subalgebra of* $\mathfrak{g}$ *such that* $\bar{\theta}(\mathfrak{m}) = \mathfrak{m}$. *Then* $\mathfrak{m}$ *is reductive in* $\mathfrak{g}$ [4].

It follows from our hypothesis that $\mathfrak{m}$ is the complexification of the subalgebra $\mathfrak{m}_0=\mathfrak{m}\cap\mathfrak{u}$. But $\mathfrak{u}$ being compact, $\mathfrak{m}_0$ is reductive in $\mathfrak{u}$ and so $\mathfrak{m}$ is reductive in $\mathfrak{g}$.

Let $\mathfrak{h}_0$ be a Cartan subalgebra of $\mathfrak{g}_0$ such that $\theta(\mathfrak{h}_0)=\mathfrak{h}_0$. For any (real-valued) linear function λ on $\mathfrak{h}_{\mathfrak{p}_0}=\mathfrak{h}_0\cap\mathfrak{p}_0$, let $\mathfrak{g}_{0\lambda}$ denote the space of those $X\in\mathfrak{g}_0$ for which $[H,X]=\lambda(H)X$ for all $H\in\mathfrak{h}_{\mathfrak{p}_0}$. Let $\mathfrak{m}_0$ be the orthogonal complement[6] of $\mathfrak{h}_{\mathfrak{p}_0}$ in $\mathfrak{g}_{00}$. Introduce an order [2(f), §2] in the space of linear functions on $\mathfrak{h}_{\mathfrak{p}_0}$ and put $\mathfrak{n}_0=\sum_{\lambda>0}\mathfrak{g}_{0\lambda}$. Obviously, $\mathfrak{m}_0$ and $\mathfrak{n}_0$ are subalgebras of $\mathfrak{g}_0$ and $\mathfrak{n}_0$ is nilpotent. Moreover, it follows from its definition that $\theta(\mathfrak{m}_0)=\mathfrak{m}_0$. Therefore, from Lemma 10, $\mathfrak{m}_0$ is reductive in $\mathfrak{g}_0$.

Let G be a connected Lie group with the Lie algebra $\mathfrak{g}_0$, and let K, N and $A_{\mathfrak{p}}$ be the analytic subgroups of G corresponding to $\mathfrak{k}_0$, $\mathfrak{n}_0$ and $\mathfrak{h}_{\mathfrak{p}_0}$, respectively. Put $\mathfrak{m}_{\mathfrak{p}_0}=\mathfrak{m}_0\cap\mathfrak{p}_0$.

LEMMA 11. *The mapping* $(k,X,a,n)\to k(\exp X)an$ $(k\in K, X\in\mathfrak{m}_{\mathfrak{p}_0}, a\in A_{\mathfrak{p}}, n\in N)$ *is a one-one regular analytic mapping of* $K\times\mathfrak{m}_{\mathfrak{p}_0}\times A_{\mathfrak{p}}\times N$ *onto* G.

Let M be the analytic subgroup of G corresponding to $\mathfrak{m}_0$. Since $\theta(\mathfrak{m}_0)=\mathfrak{m}_0$, it follows that $\mathfrak{m}_0=\mathfrak{m}_0\cap\mathfrak{k}_0+\mathfrak{m}_{\mathfrak{p}_0}$. Moreover, $[\mathfrak{m}_0,\mathfrak{n}_0]\subset\mathfrak{n}_0$, and therefore $\mathfrak{s}_0=\mathfrak{m}_0+\mathfrak{h}_{\mathfrak{p}_0}+\mathfrak{n}_0$ is a Lie algebra and $\mathfrak{n}_0$ is an ideal in $\mathfrak{s}_0$. Hence $S=MA_{\mathfrak{p}}N$ is a group and N is normal in S. Let $M_{\mathfrak{p}}$ denote the subset of M consisting of elements of the form $\exp X$ $(X\in\mathfrak{m}_{\mathfrak{p}_0})$. First we shall show that $G=KM_{\mathfrak{p}}A_{\mathfrak{p}}N$. Extend $\mathfrak{h}_{\mathfrak{p}_0}$ to a maximal abelian subspace $\mathfrak{a}_{\mathfrak{p}_0}$ of $\mathfrak{p}_0$. Let $\bar{\mathfrak{F}}$ and $\mathfrak{F}$ be the spaces of (real-valued) linear functions on $\mathfrak{a}_{\mathfrak{p}_0}$ and $\mathfrak{h}_{\mathfrak{p}_0}$, respectively. Select an order on $\bar{\mathfrak{F}}$ compatible with the one already chosen on $\mathfrak{F}$ (see Section 2). Let $\bar{\mathfrak{g}}_{0\lambda}$ $(\lambda\in\bar{\mathfrak{F}})$ denote the set of those $X\in\mathfrak{g}_0$ for which $[H,X]=\lambda(H)X$ for all $H\in\mathfrak{a}_{\mathfrak{p}_0}$. Then if $\bar{\mathfrak{n}}_0=\sum_{\lambda>0}\bar{\mathfrak{g}}_{0\lambda}$, it is clear that $\bar{\mathfrak{n}}_0$ is a nilpotent subalgebra of $\mathfrak{g}_0$ containing $\mathfrak{n}_0$. Let A_+ and $\bar{N}$ be the analytic subgroups of G corresponding to $\mathfrak{a}_{\mathfrak{p}_0}$ and $\bar{\mathfrak{n}}_0$, respectively. Then Iwasawa [3] has shown that $G=KA_+\bar{N}$. Moreover, in view of the above compatibility, it is clear that $\mathfrak{a}_{\mathfrak{p}_0}+\bar{\mathfrak{n}}_0\subset\mathfrak{g}_{00}+\mathfrak{n}_0=\mathfrak{s}_0$. Hence $A_+\bar{N}\subset S$. Therefore $G=KA_+\bar{N}=KMA_{\mathfrak{p}}N$. Now we claim that $M=M_KM_{\mathfrak{p}}$, where $M_K=M\cap K$. This is seen as follows. Since $\mathfrak{h}_0$ is maximal abelian in $\mathfrak{g}_0$, it follows that $\mathfrak{h}_{\mathfrak{k}_0}=\mathfrak{h}_0\cap\mathfrak{k}_0$ is maximal abelian in $\mathfrak{m}_0$. Therefore the center of $\mathfrak{m}_0$ is contained in $\mathfrak{h}_{\mathfrak{k}_0}$, and, since $\mathfrak{m}_0$ is reductive, $\mathfrak{m}_0'=[\mathfrak{m}_0,\mathfrak{m}_0]$ is the orthogonal complement of this center in $\mathfrak{m}_0$. This shows that $\mathfrak{m}_0'\supset\mathfrak{m}_{\mathfrak{p}_0}$.

---

[6] Whenever we speak of orthogonality or related concepts, they are to be understood with respect to the positive-definite Hermitian form $\|X\|^2$ $(X\in\mathfrak{g})$ on $\mathfrak{g}$.

Moreover $\mathfrak{m}_0$, and therefore also $\mathfrak{m}_0'$, is invariant under θ, so that $\mathfrak{m}_0' = \mathfrak{m}_0' \cap \mathfrak{k}_0 + \mathfrak{m}_{\mathfrak{p}_0}$. This means that $\mathfrak{m}_0' \cap \mathfrak{k}_0 + (-1)^{\frac{1}{2}}\mathfrak{m}_{\mathfrak{p}_0}$ is a semisimple subalgebra of $\mathfrak{u}$, and therefore it is compact. Then if M' and M_K', respectively, are the analytic subgroups of G corresponding to $\mathfrak{m}_0'$ and $\mathfrak{m}_0' \cap \mathfrak{k}_0$, we can conclude (see Mostow [5]) that $M' = M_K' M_{\mathfrak{p}}$. Now let $\mathfrak{c}_0$ be the center of $\mathfrak{m}_0$ and D the corresponding analytic subgroup of M. Then $\mathfrak{c}_0 \subset \mathfrak{m}_0 \cap \mathfrak{k}_0$, and therefore $D \subset M \cap K$ and $M = DM'$. This proves that $M = M_K M_{\mathfrak{p}}$, and hence $G = KM_{\mathfrak{p}}A_{\mathfrak{p}}N$.

Now in order to prove that our mapping is one-one, we shall first show that $M \cap A_{\mathfrak{p}}N = \{1\}$. Suppose $m = a \exp X$ $(m \in M, a \in A_{\mathfrak{p}}, X \in \mathfrak{n}_0)$. Then if[7] $b \in A_{\mathfrak{p}}$,

$$m = bmb^{-1} = a \exp \mathrm{Ad}(b)X.$$

Since the exponential mapping is well known to be one-one on $\bar{\mathfrak{n}}_0$, it follows that $X = \mathrm{Ad}(b)X$ for all $b \in A_{\mathfrak{p}}$. This implies that $[H, X] = 0$ $(H \in \mathfrak{h}_{\mathfrak{p}_0})$, and hence $X \in \mathfrak{n}_0 \cap (\mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{m}_0) = \{0\}$. Therefore $m = a$. Let $\exp \mathfrak{p}_0$ denote the set of all elements of the form $\exp Y$ $(Y \in \mathfrak{p}_0)$. Then every element in G can be written *uniquely* in the form kp $(k \in K, p \in \exp \mathfrak{p}_0$, see Mostow [5]). On the other hand $M = M_K M_{\mathfrak{p}}$, and therefore if $m = kp$, we can conclude that $k \in M_K$, $p \in M_{\mathfrak{p}}$. Moreover, $a \in A_{\mathfrak{p}} \subset \exp \mathfrak{p}_0$. Therefore $k = 1$ and $p \in M_{\mathfrak{p}} \cap A_{\mathfrak{p}}$. But again, since the exponential mapping is one-one on $\mathfrak{p}_0$, $p = \exp Y$, where $Y \in \mathfrak{m}_{\mathfrak{p}_0} \cap \mathfrak{h}_{\mathfrak{p}_0} = \{0\}$. This proves that $m = 1$. Now suppose $k \in K \cap S$. Then $k = man$ $(m \in M, a \in A_{\mathfrak{p}}, n \in N)$, and $\mathrm{Ad}(k)$ leaves $\mathfrak{n}_0$ invariant. But $\mathrm{Ad}(k) = \theta\,\mathrm{Ad}(k)\theta^{-1}$, and therefore $\mathrm{Ad}(k)$ also leaves $\theta(\mathfrak{n}_0) = \sum_{\mu<0} \mathfrak{g}_{0\mu}$ invariant. This implies that $\mathrm{Ad}(n) = \mathrm{Ad}(a^{-1}m^{-1}k)$ leaves $\theta(\mathfrak{n}_0)$ invariant. However, this is possible only if $n = 1$ as follows from Lemma 13 below. Hence $k = ma$. Now let $m = m_1 p$, where $m_1 \in M_K, p \in M_{\mathfrak{p}}$. Since $\mathfrak{h}_{\mathfrak{p}_0}$ and $\mathfrak{m}_0$ commute, $m_1^{-1}k = pa \in K \cap (\exp \mathfrak{p}_0) = \{1\}$, and so $a = p^{-1}$. But $\mathfrak{m}_{\mathfrak{p}_0} \cap \mathfrak{h}_{\mathfrak{p}_0} = \{0\}$ and so $M_{\mathfrak{p}} \cap A_{\mathfrak{p}} = \{1\}$. Therefore $a = p^{-1} = 1$, and this proves that $k = m_1 \in M_K$. Hence $K \cap S = M_K$. Let us now assume that $k_1 m_1 a_1 n_1 = k_2 m_2 a_2 n_2$ $(k_i \in K, m_i \in M_{\mathfrak{p}}, a_i \in A_{\mathfrak{p}}, n_i \in N, i = 1, 2)$. Put $m_i a_i n_i = s_i$. Then $k_1^{-1}k_2 \in K \cap S = M_K$, and therefore $k_2 = k_1 m$, where $m \in M_K$. Then $m_1^{-1}(mm_2) \in M \cap A_{\mathfrak{p}}N = \{1\}$. Hence $mm_2 = m_1$. But since both $m_1, m_2 \in M_{\mathfrak{p}} \subset \exp \mathfrak{p}_0$ and $m \in M_K \subset K$, it follows that $m = 1$ and $m_2 = m_1$. This proves that $k_1 = k_2$. Also one knows (see Iwasawa [3]) that the mapping $(a, n) \rightarrow an$ $(a \in A_+, n \in \bar{N})$ is one-one. Hence $a_1 = a_2$, $n_1 = n_2$, and this proves that the mapping of Lemma 11 is one-one.

---

[7] $x \rightarrow \mathrm{Ad}(x)$ $(x \in G)$ denotes, as usual, the adjoint representation of G.

The proof of the regularity is straightforward and we shall only sketch it here. Let ϕ denote our mapping. In order to prove that ϕ is regular at (k, X, a, n) $(k \in K, X \in \mathfrak{m}_{\mathfrak{p}_0}, a \in A_{\mathfrak{p}}, n \in N)$, we have to verify that the following linear mapping D of $\mathfrak{g}_0$ is nonsingular.[8]

$$DZ = Z \quad (Z \in \mathfrak{n}_0), \qquad DH = \mathrm{Ad}(n^{-1})H \quad (H \in \mathfrak{h}_{\mathfrak{p}_0}),$$

$$DY = \mathrm{Ad}(n^{-1}a^{-1})\{(1 - \exp(-\mathrm{ad}\,X))/\mathrm{ad}\,X\}Y \qquad (Y \in \mathfrak{m}_{\mathfrak{p}_0}),$$

$$DU = \mathrm{Ad}(n^{-1}a^{-1})\exp(-\mathrm{ad}\,X)U \qquad (U \in \mathfrak{k}_0).$$

Put $D' = \exp(\mathrm{ad}\,X)\mathrm{Ad}(an)D$. Then since $\mathfrak{g}_0$ is semisimple, it is clear that $\det D = \det D'$. Moreover, if I is the identity mapping of $\mathfrak{g}_0$, $\mathrm{Ad}(n) - I$ is nilpotent, and so the restriction of $\mathrm{Ad}(n)$ on $\mathfrak{n}_0$ has determinant 1. Similarly, since $X \in \mathfrak{m}_{\mathfrak{p}_0} \subset \mathfrak{m}_0'$, the restriction of $\exp(\mathrm{ad}\,X)$ on $\mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{n}_0$ also has determinant 1. Hence if D_1 is the linear mapping of $\mathfrak{g}_0/(\mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{n}_0)$ defined by D', $\det D = \det \mathrm{Ad}_{\mathfrak{n}_0}(a) \det D_1$, where $\mathrm{Ad}_{\mathfrak{n}_0}(a)$ is the restriction of $\mathrm{Ad}(a)$ on $\mathfrak{n}_0$. But D_1 leaves every element in $\mathfrak{k}_0 \bmod (\mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{n}_0)$ fixed. Hence it defines a linear mapping D_2 of $\mathfrak{g}_0/(\mathfrak{k}_0 + \mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{n}_0)$ and $\det D_1 = \det D_2$. On the other hand, it is clear that

$$\mathfrak{g}_0 = \mathfrak{g}_{00} + \sum_{\lambda>0} \mathfrak{g}_{0\lambda} + \sum_{\mu<0} \mathfrak{g}_{0\mu} = \mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{m}_0 + \mathfrak{n}_0 + \theta(\mathfrak{n}_0).$$

Moreover, if $Z \in \mathfrak{n}_0$, then $\theta(Z) = (\theta(Z) + Z) - Z \in \mathfrak{k}_0 + \mathfrak{n}_0$, and so $\mathfrak{n}_0 + \theta(\mathfrak{n}_0) \subset \mathfrak{k}_0 + \mathfrak{n}_0$. Therefore $\mathfrak{g}_0 = \mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{m}_{\mathfrak{p}_0} + \mathfrak{k}_0 + \mathfrak{n}_0$. We claim this sum is direct. For suppose $U \in \mathfrak{k}_0 \cap (\mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{m}_{\mathfrak{p}_0} + \mathfrak{n}_0)$. Then

$$U = \theta(U) \in (\mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{m}_{\mathfrak{p}_0} + \mathfrak{n}_0) \cap (\mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{m}_{\mathfrak{p}_0} + \theta(\mathfrak{n}_0)) = \mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{m}_{\mathfrak{p}_0}.$$

Hence $U \in \mathfrak{k}_0 \cap (\mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{m}_{\mathfrak{p}_0}) \subset \mathfrak{k}_0 \cap \mathfrak{p}_0 = \{0\}$. Therefore we may identify $\mathfrak{g}_0/(\mathfrak{k}_0 + \mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{n}_0)$ with $\mathfrak{m}_{\mathfrak{p}_0}$ in the obvious way. If $Y \in \mathfrak{m}_{\mathfrak{p}_0}$,

$$D'Y = \{(\exp(\mathrm{ad}\,X) - 1)/\mathrm{ad}\,X\}Y \equiv (\sinh \mathrm{ad}\,X/\mathrm{ad}\,X)Y \bmod \mathfrak{k}_0.$$

Therefore it is clear that

$$\det D = \det(\sinh \mathrm{ad}\,X/\mathrm{ad}\,X)_{\mathfrak{m}_{\mathfrak{p}_0}} \det \mathrm{Ad}_{\mathfrak{n}_0}(a)$$

(where the suffix $\mathfrak{m}_{\mathfrak{p}_0}$ denotes restriction on $\mathfrak{m}_{\mathfrak{p}_0}$). Since $\mathrm{Ad}(a)$ and $\sinh \mathrm{ad}\,X/\mathrm{ad}\,X$ are positive-definite self-adjoint operators on $\mathfrak{g}$, it follows that $\det D > 0$, and therefore ϕ is regular. In fact, the following lemma is an immediate consequence of the above computation.

---

[8] $\{(1 - \exp(-\mathrm{ad}\,X))/\mathrm{ad}\,X\}$ and $\sinh \mathrm{ad}\,X/\mathrm{ad}\,X$ are defined in the usual way by means of their convergent power series.

LEMMA 12. *Let dk, da, dn and dx denote the Haar measures on K, $A_{\mathfrak{p}}$, N and G, respectively, and dX the Euclidean measure on $\mathfrak{m}_{\mathfrak{p}_0}$. Then it is possible to normalize them in such a way that*

$$dx = \det(\sinh \operatorname{ad} X/\operatorname{ad} X)_{\mathfrak{m}_{\mathfrak{p}_0}} \det \operatorname{Ad}_{\mathfrak{n}_0}(a)\, dk\,da\,dn\,dX,$$

where $x = k(\exp X)an$ $(k \in K, X \in \mathfrak{m}_{\mathfrak{p}_0}, a \in A_{\mathfrak{p}_0}, n \in N)$.

The following corollary is now obvious from Lemmas 11 and 12.

COROLLARY. *The mapping* $(k, X, n, a) \rightarrow k(\exp X)na$ *is also a one-one regular mapping of* $K \times \mathfrak{m}_{\mathfrak{p}_0} \times N \times A_{\mathfrak{p}}$ *onto* G, *and if* $x = k(\exp X)na$,

$$dx = \det(\sinh \operatorname{ad} X/\operatorname{ad} X)_{\mathfrak{m}_{\mathfrak{p}_0}}\, dk\,dX\,dn\,da$$

with the same normalization of the measures as in Lemma 12.

In order to complete the proof of Lemma 11, we still have to prove the following result.

LEMMA 13. *Let X be an element in $\mathfrak{n}_0$ such that $\theta(\mathfrak{n}_0)$ is invariant under* $\operatorname{Ad}(\exp X)$. *Then* $X = 0$.

Let $\lambda_1 < \lambda_2 < \cdots < \lambda_r$ be all the positive elements $\lambda \in \mathfrak{F}$ such that $\mathfrak{g}_{0\lambda} \neq \{0\}$. Then if $X \neq 0$, let i be the largest index $(1 \leqq i \leqq r)$ such that $X \in \sum_{j \geqq i} \mathfrak{g}_{0\lambda_j}$. Then $X = X_i + X_{i+1} + \cdots + X_r$, where $X_j \in \mathfrak{g}_{0\lambda_j}$ $(1 \leqq j \leqq r)$ and $X_i \neq 0$. Now it is obvious that if $Y \in \mathfrak{g}_{0\lambda_i}$,

$$\exp(\operatorname{ad} X)\theta(Y) \equiv \theta(Y) + [X_i, \theta(Y)] \bmod \mathfrak{n}_0$$

and $[X_i, \theta(Y)] \in \mathfrak{g}_{00} = \mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{m}_0$. However the left side lies in $\theta(\mathfrak{n}_0)$ by hypothesis. Therefore, since the sum $\mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{m}_0 + \mathfrak{n}_0 + \theta(\mathfrak{n}_0)$ is direct, we conclude that $[X_i, \theta(Y)] = 0$. Hence if $H \in \mathfrak{h}_{\mathfrak{p}_0}$,

$$\lambda_i(H) B(X_i, \theta(Y)) = B([H, X_i], \theta(Y)) = B(H, [X_i, \theta(Y)]) = 0.$$

Since $\lambda_i \neq 0$, we can select H such that $\lambda_i(H) \neq 0$, and thus obtain $B(X_i, \theta(Y)) = 0$. Now take $Y = X_i$. Then we get $\| X_i \|^2 = 0$, and so $X_i = 0$. This contradiction proves the lemma.

Select an order on the space of (real-valued) linear functions on $\mathfrak{h}_{\mathfrak{p}_0} + (-1)^{\frac{1}{2}} \mathfrak{h}_{\mathfrak{k}_0}$ compatible with the one already defined in $\mathfrak{F}$. Complexify $\mathfrak{h}_0$, $\mathfrak{m}_{\mathfrak{p}_0}$, $\mathfrak{n}_0$, etc., to $\mathfrak{h}$, $\mathfrak{m}_{\mathfrak{p}}$, $\mathfrak{n}$, respectively. Let P be the set of all positive roots (of $\mathfrak{g}$ with respect to $\mathfrak{h}$) under our order. For each root α, select an element $X_\alpha \neq 0$ in $\mathfrak{g}$ such that $[H, X_\alpha] = \alpha(H) X_\alpha$ for all $H \in \mathfrak{h}$. Let P_+ be the set of those $\alpha \in P$ which are not identically zero on $\mathfrak{h}_{\mathfrak{p}}$. The remaining roots in P are divided into two disjoint classes P_0 and P_- as follows. If α is a positive root which is not in P_+, then X_α lies either in $\mathfrak{p}$ or in $\mathfrak{k}$ (see [2(e), §2]), and, by definition, α is in P_0 or P_- accordingly. Then P is the disjoint union of P_+, P_0 and P_-, and it is obvious that $\mathfrak{n} = \sum_{\alpha \in P_+} CX_\alpha$. Define polynomial functions π_+, π_0 and π_- on $\mathfrak{h}$ by $\pi_+ = \prod_{\alpha \in P_+} \alpha$, $\pi_0 = \prod_{\beta \in P_0} \alpha$, $\pi_- = \prod_{\alpha \in P_-} \alpha$, and put $\pi = \pi_+\pi_0\pi_-$.

We shall now assume that G is the (connected) adjoint group of $\mathfrak{g}_0$. Let A be the Cartan subgroup [2(e), §2] of G corresponding to $\mathfrak{h}_0$. Then $A = A_K A_{\mathfrak{p}}$, where $A_K = A \cap K$ (Lemma 7 of [2(e)]). Let $x \rightarrow x^*$ denote the natural mapping of G on the factor space $G^* = G/A$. We put $x^*H = xH$ for $x \in G$ and $H \in \mathfrak{h}$. Since K is compact, we can normalize dk in such a way that $\int_K dk = 1$. Let dm denote the Haar measure on M and dx^* the invariant measure on G^*.

LEMMA 14. *It is possible to normalize dm and dx^* in such a way that*

$$\int_{G^*} f(x^*)\,dx^* = \int_{K\times M\times N} f((kmn)^*)\,dk\,dm\,dn$$

for $f \in C_c(G^*)$.

It is clear that if the Haar measure db on A is suitably normalized, then

$$\int g(x)\,dx = \int_{G^*} dx^* \int_A g(xb)\,db \qquad (g \in C_c(G)).$$

On the other hand, from the Corollary to Lemma 12,

$$\int g(x)\,dx = \int g(k \exp Xna)s(X)\,dk\,dX\,dn\,da,$$

where $s(X) = \det(\sinh \operatorname{ad} X/\operatorname{ad} X)_{\mathfrak{m}_{\mathfrak{p}_0}}$ $(X \in \mathfrak{m}_{\mathfrak{p}_0})$. Normalize the Haar measure dm' on $M_K = M \cap K$ in such a way that $\int dm' = 1$. Then it is well known (see [2(g), §12]) that dm can be so normalized that $dm = s(X)\,dm'\,dX$, where $m = m' \exp X$ $(m' \in M_K, X \in \mathfrak{m}_{\mathfrak{p}_0})$. Therefore it is obvious that

$$\int g(k \exp Xna)s(X)\,dk\,dX\,dn\,da = \int g(kmna)\,dk\,dm\,dn\,da.$$

On the other hand, $db = c\,da'\,da$ $(b = a'a, a' \in A_K, a \in A_{\mathfrak{p}})$, where c is a positive constant and da' is the Haar measure on A_K $(\int da' = 1)$. Therefore, since $a'Ma'^{-1} = M$, $a'Na'^{-1} = N$ $(a' \in A_K)$, it is clear that

$$c\int g(kmna)\,dkdmdnda=\int_{K\times M\times N}dkdmdn\int_A g(kmnb)\,db.$$

Hence

$$c\int_{G^*}dx^*\int_A g(xb)\,db=\int_{K\times M\times N}dkdmdn\int_A g(kmnb)\,db$$

for $g\in C_c(G)$. Now suppose $f\in C_c(G^*)$. Then we can select (see Weil [7, p. 43]) $g\in C_c(G)$ such that

$$f(x^*)=\int_A g(xb)\,db \qquad (x\in G).$$

Hence

$$\int_{G^*}f(x^*)\,dx^*=c^{-1}\int_{K\times M\times N}f((kmn)^*)\,dkdmdn,$$

and this proves our assertion.

COROLLARY. *With the normalizations of Lemma* 14 *we also have*

$$\int_{G^*}f(x^*)\,dx^*=\int_{K\times M\times N}f((knm)^*)\,dkdndm$$

for $f\in C_c(G^*)$.

Since $[\mathfrak{m}_0,\mathfrak{n}_0]\subset\mathfrak{n}_0$, it follows that $mNm^{-1}=N$ $(m\in M)$. Therefore, in order to prove the corollary, it is sufficient to show that $|\det\mathrm{Ad}_{\mathfrak{n}}(m)|=1$ $(m\in M)$, where $\mathrm{Ad}_{\mathfrak{n}}(m)$ is the restriction of $\mathrm{Ad}(m)$ on $\mathfrak{n}$. Let $m=m_1m_2$ $(m_1\in M_K, m_2\in M_{\mathfrak{p}})$. Since M_K is compact and $\mathfrak{m}_{\mathfrak{p}_0}\subset[\mathfrak{m}_0,\mathfrak{m}_0]$, it follows that $|\det\mathrm{Ad}_{\mathfrak{n}}(m_1)|=\det\mathrm{Ad}_{\mathfrak{n}}(m_2)=1$, and therefore

$$|\det\mathrm{Ad}_{\mathfrak{n}}(m)|=|\det\mathrm{Ad}_{\mathfrak{n}}(m_1)\det\mathrm{Ad}_{\mathfrak{n}}(m_2)|=1.$$

Put $\mathfrak{l}_0=\mathfrak{h}_{\mathfrak{p}_0}+\mathfrak{m}_0$. Then $\mathfrak{l}_0$ is a Lie algebra which, by Lemma 10, is reductive in $\mathfrak{g}_0$. Let $\mathfrak{l}$ denote the complexification of $\mathfrak{l}_0$ in $\mathfrak{g}$ and $\zeta(L)$ $(L\in\mathfrak{l})$ the determinant of the restriction of $\mathrm{ad}\,L$ on $\mathfrak{n}$. It is obvious that ζ is a polynomial function on $\mathfrak{l}$ which takes only real values on $\mathfrak{l}_0$.

LEMMA 15. *It is possible to normalize the Euclidean measure dZ on $\mathfrak{n}_0$ so that the following condition is fulfilled. If L is an element in $\mathfrak{l}_0$ such that $\zeta(L)\neq0$, then*

$$\int_N f(nL)\,dn=|\zeta(L)|^{-1}\int_{\mathfrak{n}_0}f(L+Z)\,dZ \qquad (f\in C_c(\mathfrak{l}_0+\mathfrak{n}_0)).$$

COROLLARY. *Let H be an element in $\mathfrak{h}_0$ such that $\pi_+(H)\neq0$. Then*

$$\int|f(x^*H)|\,dx^*=|\zeta(H)|^{-1}\int|f(k(mH+Z))|\,dkdmdZ$$

for $f\in C_c(\mathfrak{g}_0)$.

It is clear that $\zeta(mH)=\zeta(H)=\pi_+(H)$ $(m\in M)$. Our corollary is therefore an immediate consequence of Lemma 15 and the Corollary of Lemma 14. On the other hand, since $[\mathfrak{l}_0,\mathfrak{n}_0]\subset\mathfrak{n}_0$, it is clear that $nL-L\in\mathfrak{n}_0$ for $n\in N$ and $L\in\mathfrak{l}_0$. Therefore Lemma 15 follows from the result below.

LEMMA 16. *Let L be an element in $\mathfrak{l}_0$ such that $\zeta(L)\neq 0$. Then the mapping $Z\rightarrow\exp(\operatorname{ad}Z)L-L$ $(Z\in\mathfrak{n}_0)$ is a one-one regular mapping of $\mathfrak{n}_0$ onto itself.*

Let ϕ denote this mapping. Then in order to show that ϕ is regular at a point $Z\in\mathfrak{n}_0$, we have to consider the endomorphism D of $\mathfrak{n}_0$ given by

$$DY=-(\operatorname{ad}L)\{(1-\exp(-\operatorname{ad}Z))/\operatorname{ad}Z\}Y \qquad (Y\in\mathfrak{n}_0)$$

and prove that $\det D\neq 0$. But since $\operatorname{ad}Z$ is nilpotent, it is clear that

$$|\det D|=|\zeta(L)|\neq 0,$$

and so ϕ is everywhere regular. Moreover, it is well known that $Z\rightarrow\exp Z$ is a one-one mapping of $\mathfrak{n}_0$ onto N. Therefore if $\exp(\operatorname{ad}Z)L=L$ $(Z\in\mathfrak{n}_0)$, it follows that $\exp(t\operatorname{ad}L)Z=Z$ $(t\in R)$, and therefore $[L,Z]=0$. But since $\zeta(L)\neq 0$, this implies that $Z=0$. This proves that $nL\neq L$ $(n\in N)$ unless $n=1$, and therefore $\phi(Z_1)=\phi(Z_2)$ $(Z_1,Z_2\in\mathfrak{n}_0)$ unless $Z_1=Z_2$. Hence ϕ is univalent.

We have still to prove that $\phi(\mathfrak{n}_0)=\mathfrak{n}_0$. Since $\mathfrak{n}_0$ is connected, it would be enough to show that $\phi(\mathfrak{n}_0)$ is closed in $\mathfrak{n}_0$. This however is an immediate consequence of the following statement. *Suppose Z varies in $\mathfrak{n}$ in such a way that $\|\exp(\operatorname{ad}Z)L-L\|$ remains bounded. Then $\|Z\|$ also remains bounded.* This is proved as follows. Since $CL+Z$ is a solvable Lie algebra over the complex field, we can choose a base $Z_1,\cdots,Z_r$ for $\mathfrak{n}$ over C and complex numbers $c_1,\cdots,c_r$ such that $[L,Z_i]\equiv c_iZ_i \bmod \sum_{k>i}CZ_k$ and $[Z_i,Z_j]\in\sum_{k>j}CZ_k$ $(1\leqq i\leqq j\leqq r)$. Moreover $c_i\neq 0$ since $\zeta(L)\neq 0$. Let $t_1,\cdots,t_r$ denote the complex Cartesian coordinates in $\mathfrak{n}$ corresponding to this base. Then it is clear that for any integer j $(1\leqq j\leqq r)$, there exists a polynomial p_j in $(j-1)$ variables $\tau_1,\cdots,\tau_{j-1}$ with complex coefficients such that

$$t_j((\exp\operatorname{ad}Z)L-L)=-c_jt_j(Z)+p_j(t_1(Z),\cdots,t_{j-1}(Z))$$

for $Z\in\mathfrak{n}$. Hence it follows by induction on j that if $\|(\exp\operatorname{ad}Z)L-L\|$ remains bounded, the same holds for $|t_j(Z)|$. This proves our statement and therefore also the lemma.

In view of the fact that $|\det D| = |\zeta(L)|$, Lemma 15 is now obvious

Let $\mathfrak{q}_0$ be any subalgebra of $\mathfrak{g}_0$ such that $\theta(\mathfrak{q}_0) = \mathfrak{q}_0$, and let $\mathfrak{q}$ be the complexification of $\mathfrak{q}_0$ in $\mathfrak{g}$. It is obvious that the fundamental bilinear form B is nondegenerate on $\mathfrak{q}$, and we know that $\mathfrak{q}$ is reductive in $\mathfrak{g}$ (Lemma 10). For any $p \in S(\mathfrak{g})$, let $p_{\mathfrak{q}}$ denote the restriction of p on $\mathfrak{q}$. Moreover, if $\mathfrak{q}_0'$ is a nonempty open subset of $\mathfrak{q}_0$, consider the space $\mathscr{S}(\mathfrak{q}_0')$ of functions $f \in C^\infty(\mathfrak{q}_0')$ such that

$$\nu_m(df;\mathfrak{q}_0') = \sup_{X \in \mathfrak{q}_0'} |f(X;d)|(1 + \|X + \theta(X)\|)^m < \infty$$

for every $d \in \partial(S(\mathfrak{q}))$ and every integer $m \geqq 0$. We define a topology in $\mathscr{S}(\mathfrak{q}_0')$ by means of these seminorms $f \rightarrow \nu_m(df;\mathfrak{q}_0')$ $(m \geqq 0, d \in \partial(S(\mathfrak{q})))$. In this way, $\mathscr{S}(\mathfrak{q}_0')$ becomes a locally convex space. Similarly, put $\tau_m(df;\mathfrak{q}_0') = \sup_{X \in \mathfrak{q}_0'} |f(X;d)|(1 + \|X\|)^m$ for $d \in \mathfrak{D}(\mathfrak{q})$ and $f \in \mathscr{C}(\mathfrak{q}_0')$. We note that

$$\nu_m(df;\mathfrak{q}_0') \leqq 2^m \tau_m(df;\mathfrak{q}_0') \qquad (d \in \partial(S(\mathfrak{q}))$$

since $\|X + \theta(X)\| \leqq \|X\| + \|\theta(X)\| = 2\|X\|$ $(X \in \mathfrak{g}_0)$.

LEMMA 17. *For any* $f \in \mathscr{S}(\mathfrak{g}_0)$, *let* g_f *denote the function on* $\mathfrak{l}_0$ *given by*

$$g_f(L) = \int_{\mathfrak{n}_0} f(L+Z)\,dZ \qquad (L \in \mathfrak{l}_0).$$

Then $g_f \in \mathscr{S}(\mathfrak{l}_0)$ *and* $f \rightarrow g_f$ *is a continuous mapping of* $\mathscr{S}(\mathfrak{g}_0)$ *into* $\mathscr{S}(\mathfrak{l}_0)$. *Moreover* $g_{\partial(p)f} = \partial(p_{\mathfrak{l}})g_f$ *for* $p \in I(\mathfrak{g})$. *Finally, if* $f \in \mathscr{C}(\mathfrak{g}_0)$ *then* $g_f \in \mathscr{C}(\mathfrak{l}_0)$ *and* $f \rightarrow g_f$ $(f \in \mathscr{C}(\mathfrak{g}_0))$ *is a continuous mapping of* $\mathscr{C}(\mathfrak{g}_0)$ *into* $\mathscr{C}(\mathfrak{l}_0)$.

Notice that $\mathfrak{l}$, $\mathfrak{n}$ and $\theta(\mathfrak{n})$ are mutually orthogonal subspaces of $\mathfrak{g}$. Hence $\|L + Z + \theta(L+Z)\|^2 = \|L + \theta(L)\|^2 + 2\|Z\|^2$ $(L \in \mathfrak{l}_0, Z \in \mathfrak{n}_0)$. Hence if $d \in \partial(S(\mathfrak{l}))$,

$$\begin{aligned}(1 + \|Z\|)^m |f(L+Z;d)| &\leqq (1 + \|L + Z + \theta(L+Z)\|)^m |f(L+Z;d)| \\ &\leqq \nu_m(df;\mathfrak{g}_0).\end{aligned}$$

We can obviously choose m so large that $\int (1 + \|Z\|)^{-m} dZ < \infty$. This shows that

$$\int_{\mathfrak{n}_0} |f(L+Z;d)|\,dZ \leqq \nu_m(df;\mathfrak{g}_0) \int (1 + \|Z\|)^{-m} dZ.$$

Hence the integral

$$\int_{\mathfrak{n}_0} f(L+Z;d)\,dZ$$

converges uniformly with respect to $L \in \mathfrak{l}_0$, and therefore g_f is of class C^∞ and

$$g_f(L;d) = \int_{\mathfrak{n}_0} f(L+Z;d)\,dZ.$$

Moreover, it is obvious that

$$\nu_{m_1}(dg_f;\mathfrak{l}_0) \leqq \nu_{m+m_1}(df;\mathfrak{g}_0) \int_{\mathfrak{n}_0} (1+\|Z\|)^{-m} dZ \qquad (m_1 \geqq 0).$$

Therefore $g_f \in \mathcal{S}(\mathfrak{l}_0)$ and the mapping $f \rightarrow g_f$ of $\mathcal{S}(\mathfrak{g}_0)$ into $\mathcal{S}(\mathfrak{l}_0)$ is continuous.

Now let f be a fixed element in $\mathcal{S}(\mathfrak{g}_0)$ and Ω a compact subset in $\mathfrak{g}_0$. For any $d \in \partial(S(\mathfrak{g}))$ and $Y \in \Omega$, consider the integral,

$$\int_{\mathfrak{n}_0} |f(Y+Z;d)|\,dZ.$$

Then

$$\|Z\| \leqq \|Z+\theta(Z)\| \leqq \|Z+Y+\theta(Z+Y)\| \\ + \|Y+\theta(Y)\| \leqq \|X+\theta(X)\| + 2a \qquad (Y \in \Omega),$$

where $X = Y+Z$ and $a = \sup_{Y \in \Omega} \|Y\|$. Hence

$$(1+\|Z\|)^m |f(Y+Z;d)| \leqq (1+2a)^m \nu_m(df;\mathfrak{g}_0),$$

and this proves that the above integral converges uniformly with respect to $Y \in \Omega$. Now put

$$g(Y) = \int_{\mathfrak{n}_0} f(Y+Z)\,dZ \qquad (Y \in \mathfrak{g}_0).$$

Then it follows from the above result that $g \in C^\infty(\mathfrak{g}_0)$ and

$$g(Y;d) = \int_{\mathfrak{n}_0} f(Y+Z;d)\,dZ \qquad (d \in \partial(S(\mathfrak{g})), Y \in \mathfrak{g}_0).$$

But it is clear that $g(Y+Z) = g(Y)$ $(Z \in \mathfrak{n}_0)$. Therefore $dg = 0$ for $d \in \partial(S(\mathfrak{g})\mathfrak{n})$. Therefore, in order to prove the second statement of the lemma, it is enough to show that $p - p_{\mathfrak{l}} \in S(\mathfrak{g})\mathfrak{n}$ for $p \in I(\mathfrak{g})$. This will be done in Lemma 18 below.

Now suppose $f \in \mathscr{C}(\mathfrak{g}_0)$. Then since $\max(\|L\|, \|Z\|) \leqq \|L+Z\|$ $(L \in \mathfrak{l}_0, Z \in \mathfrak{n}_0)$,

$$(1+\|Z\|)^m (1+\|L\|)^{m_1} |f(L+Z;d)| \leqq \tau_{m+m_1}(df;\mathfrak{g}_0)$$

for $d \in \partial(S(\mathfrak{l}))$ and $m, m_1 \geqq 0$. Hence

$$\tau_{m_1}(dg_f;\mathfrak{l}_0) \leqq \tau_{m+m_1}(df;\mathfrak{g}_0) \int_{\mathfrak{n}_0} (1+\|Z\|)^{-m} dZ,$$

and this proves that $g_f \in \mathcal{C}(\mathfrak{l}_0)$ and $f \rightarrow g_f$ is a continuous mapping of $\mathcal{C}(\mathfrak{g}_0)$ into $\mathcal{C}(\mathfrak{l}_0)$.

For any $X \in \mathfrak{g}$, let d_X denote the derivation of $S(\mathfrak{g})$ which coincides with $\operatorname{ad} X$ on $\mathfrak{g}$.

LEMMA 18. *Let p be an element in $S(\mathfrak{g})$ such that $d_H p = 0$ for $H \in \mathfrak{h}_{\mathfrak{p}}$. Then $p - p_{\mathfrak{l}} \in S(\mathfrak{g})\mathfrak{n}$.*

Let $\alpha_1, \cdots, \alpha_r$ be all the distinct roots in P_+. Then $X_{\alpha_1}, \cdots, X_{\alpha_r}$ is a base for $\mathfrak{n}$ over C. Let $\mathcal{M}$ be the set of all monomials (in $S(\mathfrak{g})$) of the form $X_{\alpha_1}{}^{m_1} \cdots X_{\alpha_r}{}^{m_r}$, where $m_1, \cdots, m_r$ are nonnegative integers. For any monomial $M = X_{\alpha_1}{}^{m_1} \cdots X_{\alpha}{}^{m_r}$, put $\beta_M = m_1\alpha_1 + \cdots + m_r\alpha_r$ and extend θ to an automorphism of $S(\mathfrak{g})$. Then it is clear that $d_H\theta(M) = -\beta_M(H)\theta(M)$ $(H \in \mathfrak{h}_{\mathfrak{p}})$. Since $\mathfrak{g}$ is the direct sum of $\mathfrak{l}$, $\mathfrak{n}$ and $\theta(\mathfrak{n})$, it follows that $S(\mathfrak{g})$ is the direct sum of $S(\mathfrak{l})S(\theta(\mathfrak{n}))$ and $S(\mathfrak{g})\mathfrak{n}$. Hence for any $q \in S(\mathfrak{g})$, there exist unique elements $q_M \in S(\mathfrak{l})$ $(M \in \mathcal{M})$ such that

$$q - \sum_M q_M \theta(M) \in S(\mathfrak{g})\mathfrak{n}.$$

Now apply d_H $(H \in \mathfrak{h}_{\mathfrak{p}})$ to this relation. Then

$$d_H q + \sum_M q_M \beta_M(H)\theta(M) \in S(\mathfrak{g})\mathfrak{n}$$

since $[\mathfrak{h}_{\mathfrak{p}}, \mathfrak{l}] = \{0\}$. In particular, if $d_H q = 0$, we get

$$\sum_M q_M \beta_M(H)\theta(M) \in S(\mathfrak{g})\mathfrak{n}.$$

But as we have observed above, $(S(\mathfrak{l})S(\theta(\mathfrak{n}))) \cap (S(\mathfrak{g})\mathfrak{n}) = \{0\}$. Therefore we conclude that $q_M\beta_M(H) = 0$ for every $M \in \mathcal{M}$. On the other hand, if $M \neq 1$, it is obvious that the restriction of β_M on $\mathfrak{h}_{\mathfrak{p}}$ is positive in our order, and so we can select $H \in \mathfrak{h}_{\mathfrak{p}}$ such that $\beta_M(H) \neq 0$. Therefore if $q = p$, we conclude that $p_M = 0$ for $M \neq 1$. This means that $p - p_1 \in S(\mathfrak{g})\mathfrak{n}$. But since $p_1 \in S(\mathfrak{l})$ and $\mathfrak{l}$ and $\mathfrak{n} + \theta(\mathfrak{n})$ are mutually orthogonal, it follows that $p_{\mathfrak{l}} = (p_1)_{\mathfrak{l}} = p_1$. Hence $p - p_{\mathfrak{l}} \in S(\mathfrak{g})\mathfrak{n}$.

COROLLARY. *Let p be an element in $S(\mathfrak{g})$ such that $d_H p = 0$ for all $H \in \mathfrak{h}_{\mathfrak{p}}$. Then $\partial(p_{\mathfrak{l}})g_f = g_{\partial(p)f}$ $(f \in \mathcal{C}(\mathfrak{g}_0))$ in the notation of Lemma 17.*

This follows immediately from Lemma 18.

Put $\pi_{\mathfrak{m}} = \pi_0\pi_-$ and let $\mathfrak{h}_0'$ be the set of all points $H \in \mathfrak{h}_0$ where $\pi(H) \neq 0$. We know that $\mathfrak{l}_0 = \mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{c}_0 + \mathfrak{m}_0'$, where $\mathfrak{c}_0$ is the center and $\mathfrak{m}_0'$ the derived algebra of $\mathfrak{m}_0$. Moreover, $\mathfrak{m}_0'$ is semisimple and $\mathfrak{m}_0' = \mathfrak{m}_0' \cap \mathfrak{k}_0 + \mathfrak{m}_{\mathfrak{p}_0}$. Finally, $\mathfrak{h}_{\mathfrak{k}_0} = \mathfrak{h}_0 \cap \mathfrak{k}_0$ is maximal abelian in $\mathfrak{m}_0$, and therefore $\mathfrak{h}_{\mathfrak{k}_0} \cap \mathfrak{m}_0'$ is a Cartan subalgebra of $\mathfrak{m}_0'$. Let D and M' be the analytic subgroups of M

corresponding to $\mathfrak{c}_0$ and $\mathfrak{m}_0'$. Then $D \subset K$ and $M = DM'$. Let $d\gamma$, dm' denote the Haar measures on D and M', respectively. We normalize them in such a way that $\int_D d\gamma = 1$ and

$$\int_M f(m)\,dm = \int_{M' \times D} f(m'\gamma)\,dm'd\gamma$$

for $f \in C_c(M)$. Now if $X \in \mathfrak{c}_0$ and $Y, Z \in \mathfrak{m}_0$, then $B(X, [Y, Z]) = B([X, Y], Z) = 0$, and from this it follows easily that $\mathfrak{c}_0$ and $\mathfrak{m}_0'$ are mutually orthogonal.[9] Moreover $\mathfrak{m}_0$ is orthogonal to $\mathfrak{h}_{\mathfrak{p}_0}$ by definition. Hence $\mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{c}_0$ is orthogonal to $\mathfrak{m}_0'$. It is clear that $X_\alpha \in \mathfrak{m}$ for $\alpha \in P_0 \cup P_-$. Therefore since $[\mathfrak{h}_\mathfrak{p} + \mathfrak{c}, \mathfrak{m}] = \{0\}$, we conclude that α vanishes identically on $\mathfrak{h}_\mathfrak{p} + \mathfrak{c}$. This proves that $\pi_\mathfrak{m}(H) = \pi_\mathfrak{m}(H_-)$ $(H \in \mathfrak{h})$, where H_- is the orthogonal projection of H in $\mathfrak{h} \cap \mathfrak{m}'$.

For any $g \in \mathcal{S}(\mathfrak{l}_0)$ and $X \in \mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{c}_0$, let g_X denote the function on $\mathfrak{m}_0'$ given by $g_X(Y) = g(X + Y)$ $(Y \in \mathfrak{m}_0')$. Then if $d \in \partial(S(\mathfrak{m}'))$, it is clear that $(dg)_X = dg_X$. Moreover since $\mathfrak{m}_0'$ and $\mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{c}_0$ are mutually orthogonal, we have

$$\nu_q(dg_X; \mathfrak{m}_0') \leqq \nu_q(dg; \mathfrak{l}_0) \qquad (q \geqq 0).$$

This proves that $g_X \in \mathcal{S}(\mathfrak{m}_0')$. Furthermore,

$$(1 + \|X + \theta(X)\|)^{q_1}(1 + \|Y + \theta(Y)\|)^{q_2} \leqq (1 + \|X + Y + \theta(X + Y)\|)^{q_1+q_2}$$

$(X \in \mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{c}_0;\ Y \in \mathfrak{m}_0';\ q_1, q_2 \geqq 0)$. Therefore

$$\sup_{X \in \mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{c}_0} (1 + \|X + \theta(X)\|)^{q_1} \nu_{q_2}(dg_X; \mathfrak{m}_0') \leqq \nu_{q_1+q_2}(dg; \mathfrak{l}_0).$$

Let $\mathfrak{h}_0''$ be the set of those points $H \in \mathfrak{h}_0$ where $\pi_0(H) \neq 0$. Then for $H \in \mathfrak{h}_0''$ and $g \in \mathcal{S}(\mathfrak{l}_0)$, consider the integral

$$\pi_\mathfrak{m}(H) \int_M g(mH)\,dm = \pi_\mathfrak{m}(H_-) \int_{M'} g_{H_0}(m'H_-)\,dm',$$

where H_0 and H_-, respectively, are the orthogonal projections of H in $\mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{c}_0$ and $\mathfrak{h}_0 \cap \mathfrak{m}_0'$. The results of Section 4 are applicable to $\mathfrak{m}_0'$ since $\mathfrak{h}_{\mathfrak{k}_0} \cap \mathfrak{m}_0'$ is maximal abelian in $\mathfrak{m}_0'$. Therefore since $g_{H_0} \in \mathcal{S}(\mathfrak{m}_0')$ and $\pi_0(H_-) = \pi_0(H) \neq 0$, the above integral is well defined. We denote its value by $\psi_g(H)$. It follows easily from Lemma 9 (applied to $\mathfrak{m}_0'$) that ψ_g is of class C^∞ on $\mathfrak{h}_0''$ and $\psi_g(H; d) = \psi_{dg}(H)$ for $d \in \partial(S(\mathfrak{h}_\mathfrak{p} + \mathfrak{c}))$. Now suppose $d_1 \in \partial(S(\mathfrak{h}_\mathfrak{p} + \mathfrak{c}))$ and $d_2 \in \partial(S(\mathfrak{h} \cap \mathfrak{m}'))$. Then $\psi_g(H; d_1 d_2) = \psi_{d_1 g}(H; d_2)$. Moreover, as we have seen during the proof of Theorem 2, we can choose an integer $N \geqq 0$, a real constant $c \geqq 1$ and a finite number of elements $d_1', \cdots, d_r' \in \partial(S(\mathfrak{m}'))$ such that

---

[9] Cf. footnote 6.

$$(1 + \| H_- \|)^{q'} | \psi_f(H; d_2) | \leqq c^{q'} \sum_{1 \leqq j \leqq r} \nu_{N+q'}(d_j' f_{H_0}; \mathfrak{m}_0')$$

for any $f \in \mathcal{D}(\mathfrak{l}_0)$, $H \in \mathfrak{h}_0''$ and $q' \geqq 0$. Therefore

$$\begin{aligned} (1 + \| H + \theta(H) \|)^{q'} & | \psi_g(H; d_1 d_2) | \\ & \leqq (1 + \| H_0 + \theta(H_0) \|)^{q'} (1 + 2 \| H_- \|)^{q'} | \psi_{d_1 g}(H; d_2) | \\ & \leqq (2c)^{q'} (1 + \| H_0 + \theta(H_0) \|)^{q'} \sum_{1 \leqq j \leqq r} \nu_{N+q'}(d_j'(d_1 g)_{H_0}; \mathfrak{m}_0') \\ & \leqq (2c)^{q'} \sum_{1 \leqq j \leqq r} \nu_{N+2q'}(d_j' d_1 g; \mathfrak{l}_0) \end{aligned}$$

since $d_j'(d_1 g)_{H_0} = (d_j' d_1 g)_{H_0}$. This proves that $\psi_g \in \mathcal{D}(\mathfrak{h}_0'')$ and the mapping $g \rightarrow \psi_g$ of $\mathcal{D}(\mathfrak{l}_0)$ into $\mathcal{D}(\mathfrak{h}_0'')$ is continuous. Let $I(\mathfrak{l})$ denote the set of all elements in $S(\mathfrak{l})$ which are invariant under M. Then it follows from Theorem 1 (applied to $\mathfrak{m}_0'$) that $\psi_{\partial(p)g} = \partial(\bar{p})\psi_g$ $(p \in I(\mathfrak{l}), g \in \mathcal{D}(\mathfrak{l}_0))$. Finally, suppose $g \in \mathcal{C}(\mathfrak{l}_0)$. Then

$$\begin{aligned} (1 + \| H \|)^{q'} & | \psi_g(H; d_1 d_2) | \\ & \leqq (1 + \| H_0 \|)^{q'} (1 + \| H_- \|)^{q'} | \psi_{d_1 g}(H; d_2) | \\ & \leqq c^{q'} (1 + \| H_0 \|)^{q'} \sum_{1 \leqq j \leqq r} \nu_{N+q'}(d_j'(d_1 g)_{H_0}; \mathfrak{m}_0') \\ & \leqq 2^{N+q'} c^{q'} \sum_{1 \leqq j \leqq r} \tau_{N+q'}(d_j' d_1 g; \mathfrak{l}_0) \end{aligned}$$

since

$$(1 + \| H_0 \|)^{q'} \tau_{N+q'}((d_j' d_1 g)_{H_0}; \mathfrak{m}_0') \leqq \tau_{N+2q'}(d_j' d_1 g; \mathfrak{l}_0).$$

This shows that in this case $\psi_g \in \mathcal{C}(\mathfrak{h}_0'')$ and $g \rightarrow \psi_g$ $(g \in \mathcal{C}(\mathfrak{l}_0))$ is a continuous mapping of $\mathcal{C}(\mathfrak{l}_0)$ into $\mathcal{C}(\mathfrak{h}_0'')$. Thus we have proved the following result.

LEMMA 19. *For any* $g \in \mathcal{D}(\mathfrak{l}_0)$, *let* ψ_g *denote the function on* $\mathfrak{h}_0''$ *defined by*

$$\psi_g(H) = \pi_{\mathfrak{m}}(H) \int_M g(mH)\, dm \qquad (H \in \mathfrak{h}_0'').$$

Then $\psi_g \in \mathcal{D}(\mathfrak{h}_0'')$ *and* $g \rightarrow \psi_g$ *is a continuous mapping of* $\mathcal{D}(\mathfrak{l}_0)$ *into* $\mathcal{D}(\mathfrak{h}_0'')$. *Moreover,* $\psi_{\partial(p)g} = \partial(\bar{p})\psi_g$ *for* $p \in I(\mathfrak{l})$ *and* $g \in \mathcal{D}(\mathfrak{l}_0)$. *Finally, if* $g \in \mathcal{C}(\mathfrak{l}_0)$, *then* $\psi_g \in \mathcal{C}(\mathfrak{h}_0'')$ *and the mapping* $g \rightarrow \psi_g$ $(g \in \mathcal{C}(\mathfrak{l}_0))$ *of* $\mathcal{C}(\mathfrak{l}_0)$ *into* $\mathcal{C}(\mathfrak{h}_0'')$ *is also continuous.*

Now for $f \in \mathcal{D}(\mathfrak{g}_0)$ and $H \in \mathfrak{h}_0'$, put

$$\phi_f(H) = \pi(H) \int_{G^*} f(x^* H)\, dx^*.$$

That this integral is well defined is seen as follows. Put

$$f_1(X) = \int_K |f(kX)|\,dk \qquad (X \in \mathfrak{g}_0).$$

Then

$$\int_{G^*} |f(x^*H)|\,dx^* = |\zeta(H)|^{-1} \int_{M\times\mathfrak{n}_0} f_1(mH + Z)\,dm\,dZ$$

from the corollary to Lemma 15. Select an integer r such that

$$c = \int_{\mathfrak{n}_0} (1 + \|Z\|)^{-r} dZ < \infty.$$

Then if $g(X) = \int_{\mathfrak{n}_0} f_1(X + Z)\,dZ \quad (X \in \mathfrak{l}_0)$,

$$(1 + \|X + \theta(X)\|)^q g(X) \leqq c\nu_{q+r}(f;\mathfrak{g}_0)$$

for any integer $q \geqq 0$. Hence by applying Lemma 7 to $\mathfrak{m}_0'$, we conclude that $\int_M g(mH)\,dm < \infty$. This proves that the above integral for ϕ_f is convergent. For any $f \in \mathscr{S}(\mathfrak{g}_0)$, let $\bar{f}$ denote the function

$$\bar{f}(X) = \int_K f(kX)\,dk \qquad (X \in \mathfrak{g}_0).$$

Since $\theta(kX) = k\theta(X)$, it is easy to see that $\bar{f} \in \mathscr{S}(\mathfrak{g}_0)$ and $f \rightarrow \bar{f}$ is a continuous mapping of $\mathscr{S}(\mathfrak{g}_0)$ into itself. (Similarly if $f \in \mathscr{C}(\mathfrak{g}_0)$, one proves easily that $\bar{f} \in \mathscr{C}(\mathfrak{g}_0)$ and $f \rightarrow \bar{f}$ $(f \in \mathscr{C}(\mathfrak{g}_0))$ is a continuous mapping of $\mathscr{C}(\mathfrak{g}_0)$ into itself). Moreover, the above calculation shows that

$$\begin{aligned}\phi_f(H) &= \pi(H)\,|\pi_+(H)|^{-1} \int_{M\times\mathfrak{n}_0} \bar{f}(mH + Z)\,dm\,dZ \\ &= \epsilon_+(H)\,\pi_{\mathfrak{m}}(H) \int_{M\times\mathfrak{n}_0} \bar{f}(mH + Z)\,dm\,dZ \qquad (f \in \mathscr{S}(\mathfrak{g}_0)),\end{aligned}$$

where $\epsilon_+(H) = 1$ or -1 according as $\pi_+(H)$ is positive[10] or negative. Put

$$\psi_f(H) = \pi_{\mathfrak{m}}(H) \int_{M\times\mathfrak{n}_0} \bar{f}(mH + Z)\,dm\,dZ \qquad (H \in \mathfrak{h}_0'', f \in \mathscr{S}(\mathfrak{g}_0)).$$

It follows from Lemmas 17 and 19 that $\psi_f \in \mathscr{S}(\mathfrak{h}_0'')$ and $f \rightarrow \psi_f$ is a continuous mapping of $\mathscr{S}(\mathfrak{g}_0)$ into $\mathscr{S}(\mathfrak{h}_0'')$. Define g_f as in Lemma 17. Then

$$\psi_f(H) = \pi_{\mathfrak{m}}(H) \int_M g_f(mH)\,dm \qquad (f \in \mathscr{S}(\mathfrak{g}_0), H \in \mathfrak{h}_0'').$$

---

[10] Notice that $\pi_+(H)$ is real since it is equal to the determinant of the restriction of ad H on $\mathfrak{n}_0$

Now suppose $p \in I(\mathfrak{g})$. If $f_1 = \partial(p)f$, it is obvious that $\bar{f}_1 = \partial(p)\bar{f}$. Hence

$$\psi_{\partial(p)f}(H) = \pi_{\mathfrak{m}}(H) \int_M g_{\bar{f}}(mH\,;\partial(p_{\mathfrak{l}}))\,dm = \psi_f(H\,;\partial(\bar{p}))$$

from Lemmas 17 and 19. Finally, if $f \in \mathscr{C}(\mathfrak{g}_0)$, we conclude from these two lemmas that $\psi_f \in \mathscr{C}(\mathfrak{h}_0'')$ and the mapping $f \to \psi_f$ $(f \in \mathscr{C}(\mathfrak{g}_0))$ of $\mathscr{C}(\mathfrak{g}_0)$ into $\mathscr{C}(\mathfrak{h}_0'')$ is continuous. Thus we have obtained the following theorem.

THEOREM 3. *For any $f \in \mathscr{D}(\mathfrak{g}_0)$, the integral*

$$\phi_f(H) = \pi(H) \int_{G^*} f(x^*H)\,dx^*$$

is absolutely convergent for $H \in \mathfrak{h}_0'$ and the function ϕ_f, so defined, lies in $\mathscr{D}(\mathfrak{h}_0')$. Moreover, $f \to \phi_f$ is a continuous mapping of $\mathscr{D}(\mathfrak{g}_0)$ into $\mathscr{D}(\mathfrak{h}_0')$, and

$$\phi_{\partial(p)f} = \partial(\bar{p})\phi_f$$

for $p \in I(\mathfrak{g})$. Let $\mathfrak{h}_0''$ be the set of those points $H \in \mathfrak{h}_0$ where $\prod_{\alpha \in P_0} \alpha(H) \neq 0$ and let $\epsilon_+(H)$ denote the sign of $\pi_+(H)$ $(H \in \mathfrak{h}_0')$. Then $\epsilon_+\phi_f$ $(f \in \mathscr{D}(\mathfrak{g}))$ can be extended to a function of class C^∞ on $\mathfrak{h}_0''$. Finally, $\phi_f \in \mathscr{C}(\mathfrak{h}_0')$ if $f \in \mathscr{C}(\mathfrak{g}_0)$, and the mapping $f \to \phi_f$ of $\mathscr{C}(\mathfrak{g}_0)$ into $\mathscr{C}(\mathfrak{h}_0')$ is also continuous.

Define the homomorphism δ of $\mathfrak{J}(\mathfrak{g})$ into $\mathfrak{J}(\mathfrak{h})$ as in Theorem 1 of [2(h)].

COROLLARY. *If $\xi \in \mathfrak{J}(\mathfrak{g})$ and $f \in \mathscr{C}(\mathfrak{g}_0)$, then $\phi_{\xi f} = \delta(\xi)\phi_f$.*

From the above theorem, this is true if $\xi \in \partial(I(\mathfrak{g}))$. Since $\mathfrak{J}(\mathfrak{g})$ is generated by $I(\mathfrak{g}) \cup \partial(I(\mathfrak{g}))$, it is enough to verify the above statement for $\xi \in I(\mathfrak{g})$. But then $\xi f \in \mathscr{C}(\mathfrak{g}_0)$, and it is obvious from the definition of ϕ_f that

$$\phi_{\xi f} = \bar{\xi}\phi_f = \delta(\xi)\phi_f.$$

6. Fourier transforms. Let dX denote the regular Euclidean measure on $\mathfrak{g}_0$ (see [2(h), §2]) and for any $f \in \mathscr{C}(\mathfrak{g}_0)$, let $\hat{f}$ denote the Fourier transform of f so that

$$\hat{f}(Y) = \int_{\mathfrak{g}_0} \exp\{(-1)^{\frac{1}{2}}B(Y,X)\}f(X)\,dX \qquad (Y \in \mathfrak{g}_0).$$

Fix an element $H_0 \in \mathfrak{h}_0'$ and consider the mapping $T_{H_0} : f \to \phi_{\hat{f}}(H_0)$ $(f \in \mathscr{C}(\mathfrak{g}_0))$. It follows from Theorem 3 that T_{H_0} is a $\mathscr{C}$-distribution. We intend to study this distribution more closely. For any $p \in S(\mathfrak{g})$, let $\hat{p}$ denote the

Furthermore, select $\beta_s \in C_c^\infty(V)$ such that

$$\int_V \exp\{(-1)^{\frac{1}{2}} B(yH_0, s\bar{H})\} \beta_s(\bar{H}) d\bar{H} = 1 \qquad (s \in \bar{W}).$$

Fix an element $\alpha \in C_c^\infty(\bar{G})$ such that $\int \alpha(\bar{x}) d\bar{x} = 1$, and define $f_s \in C_c^\infty(\mathfrak{g}_1)$ by $f_s(\bar{x}\bar{H}) = \alpha(\bar{x})\beta_s(\bar{H}; \partial(q_s))\bar{\pi}(\bar{H})^{-1} (\bar{x} \in \bar{G}, \bar{H} \in V)$. Then if $H \in U$,

$$\begin{aligned} \phi_{\bar{f}_s}(H) &= \sum_{t \in \bar{W}} c_t(H) \int \beta_s(\bar{H}; \partial(q_s)) \exp\{(-1)^{\frac{1}{2}} B(t\bar{H}, yH)\} d\bar{H} \\ &= \sum_{t \in \bar{W}} c_t(H) a_{s,t}(H) \qquad (s \in \bar{W}), \end{aligned}$$

where

$$a_{s,t}(H) = q_s(-(-1)^{\frac{1}{2}} t^{-1} yH) \int \beta_s(\bar{H}) \exp\{(-1)^{\frac{1}{2}} B(t\bar{H}, yH)\} d\bar{H}.$$

But it is clear that $a_{s,t}$ are analytic functions on U and

$$a_{s,t}(H_0) = \begin{cases} 1 & \text{if } s = t, \\ 0 & \text{if } s \neq t. \end{cases}$$

Therefore if U is sufficiently small, the determinant of the matrix $(a_{s,t})_{s,t \in \bar{W}}$ is nowhere zero on U. Let $(b_{s,t})_{s,t \in \bar{W}}$ denote the inverse matrix. Then the $b_{s,t}$ are also analytic functions on U and

$$c_t(H) = \sum_{s \in \bar{W}} b_{t,s}(H) \phi_{\bar{f}_s}(H) \qquad (H \in U)$$

Therefore since $\phi_{\bar{f}_s}$ are of class C^∞ on U (Theorem 3), the same holds for c_t.

Put

$$\sigma(H : \bar{H}) = \sum_{s \in \bar{W}} c_s(H) \exp\{(-1)^{\frac{1}{2}} B(yH, s\bar{H})\} \qquad (H \in U, \bar{H} \in V).$$

Then σ is of class C^∞ on $U \times V$. On the other hand, $\partial(p)\bar{f} = (p'f)^{-}$ $(p \in S(\mathfrak{g}), f \in C_c^\infty(\mathfrak{g}))$, and therefore if $p \in I(\mathfrak{g})$,

$$\phi_{(p'f)^{-}} = \partial(\bar{p}) \phi_{\bar{f}}$$

from Theorem 3. Select α as above and define $f \in C_c^\infty(\mathfrak{g}_1)$ by $f(\bar{x}\bar{H}) = \alpha(\bar{x})\beta(\bar{H})\bar{\pi}(\bar{H})^{-1}$ $(\beta \in C_c^\infty(V))$. Then $\bar{\phi}_f(\bar{H}) = \beta(\bar{H})$ and $\bar{\phi}_{p'f}(\bar{H}) = p'(\bar{H})\beta(\bar{H}) (\bar{H} \in V)$, and so the above equation becomes

$$\int p'(\bar{H})\beta(\bar{H})\sigma(H : \bar{H}) d\bar{H} = \int \beta(\bar{H})\sigma(H; \partial(\bar{p}) : \bar{H}) d\bar{H} \qquad (H \in U).$$

As this is true for every $\beta \in C_c^\infty(V)$, we conclude that

$$\sigma(H; \partial(\bar{p}) : \bar{H}) = p'(\bar{H})\sigma(H : \bar{H}) \qquad (p \in I(\mathfrak{g}))$$

for $H \in U$ and $\bar{H} \in V$. Thus it is enough to prove the following result.

LEMMA 23. *Suppose* c_s $(s \in \bar{W})$ *are functions of class* C^∞ *on* U *and*

$$\sigma(H:\bar{H}) = \sum_{s\in\bar{W}} c_s(H)\exp\{(-1)^{\frac{1}{2}}B(yH, s\bar{H})\} \qquad (H\in U, \bar{H}\in V).$$

Then if $\sigma(H;\partial(\bar{p}):\bar{H}) = p'(\bar{H})\sigma(H:\bar{H})$ *for all* $p \in I(\mathfrak{g})$ *and* $(H,\bar{H}) \in U\times V$, *it follows that each* c_s *is constant on* U.

Fix $\bar{H}$ in V for a moment, and let μ_s denote the linear function $H\rightarrow(-1)^{\frac{1}{2}}B(s\bar{H}, yH)$ $(H\in\mathfrak{h})$ on $\mathfrak{h}$. Since $\bar{\pi}(\bar{H})\neq 0$, the functions μ_s $(s\in W)$ are all distinct. Therefore e^{μ_s} are linearly independent over $S(\mathfrak{h})$ (Lemma 41 of [2(b)]). This means that the coefficients of e^{μ_s} in $\sigma(H;\partial(\bar{p}):\bar{H}) - p'(\bar{H})\sigma(H:\bar{H})$ must all be zero. But it is obvious that for a fixed s, this coefficient is of the form

$$c_s(H;\partial(\bar{p})) + \sum_{1\leqq i\leqq N} q_i(\bar{H})b_i(H) - p'(\bar{H})c_s(H),$$

where the q_i are certain homogeneous elements in $S(\bar{\mathfrak{h}})$ of positive degree and the b_i are functions of class C^∞ on U. Since $\bar{H}$ was an arbitrary element of V, we conclude that

$$c_s(H;\partial(\bar{p})) = 0 \qquad (s\in\bar{W}, H\in U)$$

for all homogeneous elements $p\in I(\mathfrak{g})$ of positive degree. But then it follows from Lemmas 12 and 14 of [2(h)] that c_s is a polynomial function. Now again fix $\bar{H}\in V$. Then, in view of the equation $\sigma(H;\partial(\bar{p}):\bar{H}) = p'(\bar{H})\sigma(H:\bar{H})$ $(p\in I(\mathfrak{g}))$, we conclude from the Corollary of Lemma 13 of [2(h)] that

$$\sigma(H:\bar{H}) = \sum_{s\in W} b_s e^{\mu_s(H)} \qquad (H\in U),$$

where the b_s are certain complex numbers independent of H. However the e^{μ_s} are linearly independent over $S(\mathfrak{h})$, and therefore $c_s = b_s$ $(s\in\bar{W})$. This proves that the c_s are constant on U.

Thus we have obtained the following result which should be compared with Theorem 3 of [2(h)].

LEMMA 24. *Let* $\mathfrak{h}_1$ *be a connected component of* $\mathfrak{h}_0'$. *Then there exist complex numbers* c_s $(s\in\bar{W})$ *such that*

$$\phi_{\bar{f}}(H) = \sum_{s\in\bar{W}} c_s \int \bar{\Phi}_f(\bar{H})\exp\{(-1)^{\frac{1}{2}}B(s\bar{H}, yH)\}d\bar{H} \qquad (H\in\mathfrak{h}_1)$$

for all $f\in C_c^\infty(\mathfrak{g}_1)$.

For any $X\in\mathfrak{g}_0'$, put $\epsilon(X) = 1$ or -1 according as $\eta(X)$ is positive or negative. Then it is clear that for a fixed $H \in \mathfrak{h}_1$, there exists an analytic function F_H on $\mathfrak{g}_1$ such that

$$F_H(\bar{x}\bar{H}) = \epsilon(\bar{H})\bar{\pi}(\bar{H})^{-1} \sum_{s \in \bar{W}} c_s \exp\{(-1)^{\frac{1}{2}} B(s\bar{H}, yH)\}$$

$(\bar{x} \in \bar{G}, \bar{H} \in V)$ and

$$\phi_{\bar{f}}(H) = \int f(X) F_H(X)\, dX \qquad (f \in C_c^{\infty}(\mathfrak{g}_1)).$$

(Compare this formula for F_H with Theorem 2 of [2(h)]). This shows that the distribution $f \rightarrow \phi_{\bar{f}}(H)$ coincides on $\mathfrak{g}_1$ with F_H. Thus we have proved the following theorem.

THEOREM 4. *For a fixed $H \in \mathfrak{h}_0'$ consider the $\mathscr{B}$-distribution $T_H : f \rightarrow \phi_{\bar{f}}(H)$ $(f \in \mathscr{B}(\mathfrak{g}_0))$ on $\mathfrak{g}_0$. Then T_H coincides on $\mathfrak{g}_0'$ with an analytic function F_H.*

Since T_H is invariant under G, the same holds for F_H. The exact form of F_H has already been obtained above.

7. The distributions T and T'. Let $H_1, \cdots, H_l$ be a base for $\mathfrak{h}_0$ over R. It is clear that there exists a positive constant c such that if $H = t_1H_1 + \cdots + t_lH_l$ $(t_i \in R)$, then $|t_i| \leqq c \| H \|$ $(1 \leqq i \leqq l)$. Now suppose $\mathfrak{h}_1$ is a connected component of $\mathfrak{h}_0'$ and $f \in \mathscr{B}(\mathfrak{h}_1)$. Then $\partial(H)f = \sum_{1 \leqq i \leqq l} t_i \partial(H_i)f$ and therefore

$$\nu(\partial(H)f) \leqq c \| H \| \sum_{1 \leqq i \leqq l} \nu(\partial(H_i)f) \qquad (H \in \mathfrak{h}_0),$$

where $\nu(g) = \sup_{H \in \mathfrak{h}_1} |g(H)|$ $(g \in \mathscr{B}(\mathfrak{h}_1))$. Suppose H, H' are two points in $\mathfrak{h}_1$ and the straight line-segment joining them lies entirely in $\mathfrak{h}_1$. Then if $f \in \mathscr{B}(\mathfrak{h}_1)$,

$$f(H') - f(H) = \int_0^1 (d/dt) f(H + t(H' - H))\, dt,$$

and therefore

$$|f(H') - f(H)| \leqq \nu(\partial(H' - H)f) \leqq c \| H' - H \| \sum_{1 \leqq i \leqq l} \nu(\partial(H_i)f).$$

But in view of Lemma 43 of the Appendix (§12), we can conclude that these inequalities are actually valid for any two points $H, H' \in \mathfrak{h}_1$, and so we have the following result.

LEMMA 25. *Let* Cl$(\mathfrak{h}_1)$ *denote the closure of $\mathfrak{h}_1$ in $\mathfrak{h}_0$. Then every $f \in \mathscr{B}(\mathfrak{h}_1)$ can be extended to a continuous function on* Cl$(\mathfrak{h}_1)$.

For any $\phi \in \mathscr{C}(\mathfrak{h}_0')$ and $\xi \in \mathfrak{D}(\mathfrak{h})$, put

$$\operatorname*{Lim}_{\mathfrak{h}_1} \phi(0) = \operatorname*{Lim}_{H \to 0} \phi(H), \qquad \operatorname*{Lim}_{\mathfrak{h}_1} \phi(0;\xi) = \operatorname*{Lim}_{H \to 0} \phi(H;\xi) \qquad (H \in \mathfrak{h}_1).$$

It is clear from the above corollary that these limits exist and

$$|\operatorname*{Lim}_{\mathfrak{h}_1} \phi(0;\xi)| \leqq \nu(\xi\phi).$$

Therefore for a fixed ξ, the mapping $\phi \to \operatorname*{Lim}_{\mathfrak{h}_1} \phi(0;\xi)$ is continuous on $\mathscr{C}(\mathfrak{h}_0')$. Let ξ_0 denote the local expression of ξ at zero. Then if $\xi_0 = 0$, it is obvious that $\operatorname*{Lim}_{\mathfrak{h}_1} \phi(0;\xi) = 0$. Hence

$$\operatorname*{Lim}_{\mathfrak{h}_1} \phi(0;\xi) = \operatorname*{Lim}_{\mathfrak{h}_1} \phi(0;\xi_0)$$

for $\phi \in \mathscr{C}(\mathfrak{h}_0')$ and $\xi \in \mathfrak{D}(\mathfrak{h})$.

We know from Theorem 3 that if $f \in \mathscr{C}(\mathfrak{g}_0)$, then $\phi_f \in \mathscr{C}(\mathfrak{h}_0')$. Hence we can consider the mapping $T : f \to \operatorname*{Lim}_{\mathfrak{h}_1} \phi_f(0;\partial(\pi))$ $(f \in \mathscr{C}(\mathfrak{g}_0))$. It follows immediately from Theorem 3 and what we have said above, that T is a $\mathscr{C}$-distribution.

LEMMA 26. *Define the polynomial* $\eta \in I(\mathfrak{g})$ *as in Section* 6. *Then*

$$\eta^k \partial(\eta^k) T = \langle \eta^k, \eta^k \rangle T$$

for any integer $k \geqq 0$.

Put $\xi = \partial(\eta^k) \circ \eta^k$. Then we know from the Corollary of Theorem 3 that $\phi_{\xi f} = \delta(\xi)\phi_f$ $(f \in \mathscr{C}(\mathfrak{g}_0))$, and therefore

$$T(\xi f) = \operatorname*{Lim}_{\mathfrak{h}_1} \phi_f(0;\partial(\pi) \circ \delta(\xi)) = \langle \eta^k, \eta^k \rangle T(f)$$

from the Corollary of Lemma 18 of [2(h)]. Our assertion now follows from the fact that the degree of η is even.

It is one of our principal objects to prove that $T(f) = cf(0)$ $(f \in \mathscr{C}(\mathfrak{g}_0)$, where c is a complex number independent of f. However, the proof of this fact is rather long and difficult, and we shall not be able to complete it in this paper. We consider first the Fourier transform T' of T given by $T'(f) = T(\bar{f})$ $(f \in \mathscr{C}(\mathfrak{g}_0))$. Then T' is also a $\mathscr{C}$-distribution on $\mathfrak{g}_0$, and the above-mentioned fact about T is obviously equivalent to the statement that T' coincides on $\mathfrak{g}_0$ with a constant. This we shall first prove in a weaker form. As before, let $\mathfrak{g}_0'$ denote the set of regular elements in $\mathfrak{g}_0$.

LEMMA 27. *Let* T' *be the* $\mathscr{C}$-*distribution on* $\mathfrak{g}_0$ *defined by*

$$T'(f) = \operatorname*{Lim}_{\mathfrak{h}_1} \phi_{\bar{f}}(0;\partial(\pi)) \qquad (f \in \mathscr{C}(\mathfrak{g}_0)).$$

Then on each connected component of $\mathfrak{g}_0'$, T' *coincides with a constant.*

It is obviously sufficient to prove that if $\bar{H}_0 \in \mathfrak{g}_0'$, then T' coincides on some open neighborhood of $\bar{H}_0$ in $\mathfrak{g}_0'$ with a constant. We use the notation of the proof of Lemma 24. Then

$$\phi_{\bar{f}}(H) = \sum_{s \in \bar{W}} c_s \int_V \bar{\phi}_f(\bar{H}) \exp\{(-1)^{\frac{1}{2}} B(s\bar{H}, yH)\} d\bar{H} \qquad (H \in \mathfrak{h}_1)$$

for $f \in C_c^\infty(\mathfrak{g}_1)$. Hence

$$\phi_{\bar{f}}(H; \partial(\pi)) = \sum_{s \in \bar{W}} c_s (-1)^{r/2} \int_V \bar{\phi}_f(\bar{H}) \pi(y^{-1}s\bar{H}) \exp\{(-1)^{\frac{1}{2}} B(s\bar{H}, yH)\} d\bar{H}$$

where r is the degree of π. This implies that

$$T'(f) = \sum_{s \in \bar{W}} c_s (-1)^{r/2} \int_V \bar{\phi}_f(\bar{H}) \pi(y^{-1}s\bar{H}) d\bar{H}.$$

But $\pi(y^{-1}s\bar{H})^2 = \eta(y^{-1}s\bar{H}) = \eta(\bar{H}) = \bar{\pi}(\bar{H})^2$. Therefore it is obvious that $\epsilon_s = \pi(y^{-1}s\bar{H})/\bar{\pi}(\bar{H})$ is constant for $\bar{H} \in V$. Hence

$$T'(f) = c' \int_V \bar{\pi}(\bar{H}) \bar{\phi}_f(\bar{H}) d\bar{H},$$

where $c' = \sum_{s \in \bar{W}} (-1)^{r/2} c_s \epsilon_s$. Now put $\epsilon = 1$ or -1 according as η is positive or negative on $\mathfrak{g}_1$. Then

$$\int_V \bar{\pi}(\bar{H}) \bar{\phi}_f(\bar{H}) d\bar{H} = \epsilon \int f(X) dX \qquad (f \in C_c^\infty(\mathfrak{g}_1)),$$

and therefore

$$T'(f) = c \int f(X) dX \qquad (f \in C_c^\infty(\mathfrak{g}_1))$$

if $c = c'\epsilon$. This proves that T' coincides with c on $\mathfrak{g}_1$.

LEMMA 28. *$\mathfrak{g}_0'$ has only a finite number of connected components.*

From the corollary of Lemma 2 of [2(e)], we can select a finite number of Cartan subalgebras $\mathfrak{h}_{(i)}$ $(1 \leqq i \leqq N)$ such that every Cartan subalgebra of $\mathfrak{g}_0$ is conjugate to some $\mathfrak{h}_{(i)}$ under G. Put $\mathfrak{h}_{(i)}' = \mathfrak{h}_{(i)} \cap \mathfrak{g}_0'$ and $V_i = \bigcup_{x \in G} x\mathfrak{h}_{(i)}'$. Let X be an element $\mathfrak{g}_0'$, and let $\mathfrak{h}_X$ denote the centralizer of X in $\mathfrak{g}_0$. Then since X is regular, $\mathfrak{h}_X$ is a Cartan subalgebra. Hence $\mathfrak{h}_X = x\mathfrak{h}_{(i)}$ for some $x \in G$ and some i $(1 \leqq i \leqq N)$. Therefore $X \in \mathfrak{h}_X \cap \mathfrak{g}_0' \subset V_i$, and this proves that $\mathfrak{g}_0' = V_1 \cup V_2 \cup \cdots \cup V_N$. On the other hand, we know that $\mathfrak{h}_0'$ (and therefore, similarly $\mathfrak{h}_{(i)}'$) has only a finite number of connected components. Since G is connected, it is therefore obvious that the same holds for each V_i. But this implies the statement of the lemma.

LEMMA 29. *Let $\mathfrak{g}_1, \mathfrak{g}_2, \cdots, \mathfrak{g}_N$ be all the distinct connected components of $\mathfrak{g}_0'$ and c_i the constant such that $T' = c_i$ on $\mathfrak{g}_i$ $(1 \leqq i \leqq N)$. Let Ω be an open subset of $\mathfrak{g}_0$ whose closure is compact. Then there exists an integer $k \geqq 0$ such that*

$$\langle \eta^k, \eta^k \rangle T'(f) = \sum_{1 \leqq i \leqq N} c_i \int_{\mathfrak{g}_i} \eta(X)^k f(X; \partial(\eta^k))\, dX$$

for all $f \in C_c^\infty(\Omega)$.

Let τ' denote the distribution on $\mathfrak{g}_0$ given by

$$\tau'(g) = T'(g) - \sum_{1 \leqq i \leqq N} c_i \int_{\mathfrak{g}_i} g(X)\, dX \qquad (g \in C_c^\infty(\mathfrak{g}_0)).$$

Then it is clear that the carrier of τ' is contained in the set of singular points of $\mathfrak{g}_0$. For any $f \in C_c^\infty(\Omega)$, let τ_f denote the distribution on R defined as follows:

$$\tau_f(\beta) = \tau'(\beta(\eta) f) \qquad (\beta \in C_c^\infty(R)),$$

where $\beta(\eta)$ is the function on $\mathfrak{g}_0$ whose value at $X \in \mathfrak{g}_0$ is $\beta(\eta(X))$. It is clear that no point in R other than zero, can lie in the carrier of τ_f. Moreover, since the closure of Ω is compact, τ' is of finite order on Ω (see Schwartz [6(I) pp. 82-83]). Hence there exists an integer k (independent of f) such that the order of τ_f (on R) is $< k$. This implies that $\tau'(\eta^k f) = 0$ for all $f \in C_c^\infty(\Omega)$.

For any $p \in S(\mathfrak{g})$ define $\hat{p}$ as in the proof of Lemma 20. Then obviously, $\hat{\eta}$ coincides on $\mathfrak{h}$ with $(-1)^r \pi^2$ (where r is the degree of π). Therefore it follows from Lemma 9 of [2(h)] that $\hat{\eta} = (-1)^r \eta$, and so

$$(\eta^k \partial(\eta^k) g)^{\sim} = \partial(\eta^k)(\eta^k \tilde{g}) \qquad (g \in \mathscr{B}(\mathfrak{g}_0))$$

from Lemma 1 of [2(h)]. Hence we conclude from Lemma 26 that

$$T'(\eta^k \partial(\eta^k) g) = \langle \eta^k, \eta^k \rangle T'(g).$$

Now suppose $f \in C_c^\infty(\Omega)$. Then $\tau'(\eta^k \partial(\eta^k) f) = 0$, and therefore

$$\langle \eta^k, \eta^k \rangle T'(f) = T'(\eta^k \partial(\eta^k) f) = \sum_{1 \leqq i \leqq N} c_i \int_{\mathfrak{g}_i} \eta(X)^k f(X; \partial(\eta^k))\, dX.$$

COROLLARY. *If $c_1, c_2, \cdots, c_N$ are all equal then $T' = c_1$ on $\mathfrak{g}_0$.*

It is sufficient to prove that $T' = c_1$ on Ω. But if $f \in C_c^\infty(\Omega)$, we know from the above lemma that

$$\langle \eta^k, \eta^k \rangle T'(f) = c_1 \int_{\mathfrak{g}_0} \eta(X)^k f(X; \partial(\eta^k))\, dX$$

since $c_1 = c_2 = \cdots = c_N$. Moreover, since η is a homogeneous polynomial of even degree, $\partial(\eta^k)$ is self-adjoint, and therefore

$$\int_{\mathfrak{g}_0} \eta(X)^k f(X;\partial(\eta^k))\,dX = \langle \eta^k, \eta^k \rangle \int_{\mathfrak{g}_0} f(X)\,dX.$$

On the other hand, $\langle \eta^k, \eta^k \rangle \neq 0$ (see the corollary to Lemma 18 of [2(h)]). Therefore

$$T'(f) = c_1 \int_{\mathfrak{g}_0} f(X)\,dX,$$

and this proves that $T' = c_1$ on Ω.

In view of this corollary, our main task now is to prove that the constants $c_1, \cdots, c_N$ of Lemma 29 are all equal. This will be done in another paper. However we note the following result for later use.

LEMMA 30. *Let ξ be any homogeneous polynomial in $I(\mathfrak{g})$ of positive degree. Then $\partial(\xi)T' = 0$.*

Define ξ' as in Lemma 20. Then if $f \in \mathscr{C}(\mathfrak{g}_0)$.

$$T'(\partial(\xi)f) = T((\partial(\xi)f)^{-}) = (-1)^m T(\xi'\bar{f}),$$

where m is the degree of ξ. Since $\xi' \in I(\mathfrak{g})$, it follows from Theorem 3 that $\phi_{\xi'\bar{f}} = \bar{\xi}'\phi_{\bar{f}}$, where $\bar{\xi}'$ is the restriction of ξ' on $\mathfrak{h}_0$. Therefore

$$T(\xi'\bar{f}) = \operatorname*{Lim}_{\mathfrak{h}_1} \phi_{\bar{f}}(0;\partial(\pi)\circ\bar{\xi}') = \operatorname*{Lim}_{\mathfrak{h}_1} \phi_{\bar{f}}(0;d),$$

where d is the local expression of $\partial(\pi)\circ\bar{\xi}'$ at zero. But since $m \geqq 1$, it follows from Lemma 18 of [2(h)] that $d = 0$. This proves that $\partial(\xi)T' = 0$.

8. Fundamental Cartan subalgebras.

Let ω be the Casimir polynomial of $\mathfrak{g}$ and Γ_0 a Cartan subalgebra of $\mathfrak{g}_0$. Put $l_-(\Gamma_0) = \sup_{\Gamma_1} (\dim_R \Gamma_1)$, where Γ_1 runs over all linear subspaces of Γ_0 on which ω is negative-definite. Moreover let $l_- = \sup_{\Gamma_0} l_-(\Gamma_0)$, where Γ_0 runs over all Cartan subalgebras of $\mathfrak{g}_0$. We say that Γ_0 is *fundamental* if $l_-(\Gamma_0) = l_-$. It is obvious that $l_-(x\Gamma_0) = l_-(\Gamma_0)$ $(x \in G)$. Hence if Γ_0 is fundamental, the same holds for any Cartan subalgebra conjugate to Γ_0 under G.

LEMMA 31. $l_- = \operatorname{rank} \mathfrak{k}$.

Let Γ_0 be a fundamental Cartan subalgebra of $\mathfrak{g}_0$. By going over to a conjugate subalgebra, we may assume (see the Corollary of Lemma 1 of [2(e)]) that $\theta(\Gamma_0) = \Gamma_0$. Then since ω is positive-definite on $\mathfrak{p}_0$ and negative-definite on $\mathfrak{k}_0$, it is clear that $l_- = l_-(\Gamma_0) = \dim_R(\Gamma_0 \cap \mathfrak{k}_0)$. Hence $l_- \leqq \operatorname{rank} \mathfrak{k}$. Conversely, let $\mathfrak{a}_{\mathfrak{k}_0}$ be a maximal abelian subalgebra of $\mathfrak{k}_0$. We extend it to a Cartan subalgebra $\mathfrak{a}_0$ of $\mathfrak{g}_0$. Then

$$l_- \geqq l_-(\mathfrak{a}_0) \geqq \dim_R \mathfrak{a}_{\mathfrak{k}_0} = \operatorname{rank} \mathfrak{k}.$$

This proves that $l_- = \operatorname{rank} \mathfrak{k}$.

Corollary. *Let Γ_0 be a Cartan subalgebra of $\mathfrak{g}_0$ such that $\theta(\Gamma_0) = \Gamma_0$. Then Γ_0 is fundamental if and only if $\Gamma_0 \cap \mathfrak{k}_0$ is maximal abelian in $\mathfrak{k}_0$.*

For it is obvious that $l_-(\Gamma_0) = \dim_R(\Gamma_0 \cap \mathfrak{k}_0)$, and therefore from the above lemma, $l_-(\Gamma_0) = l_-$ if and only if $\Gamma_0 \cap \mathfrak{k}_0$ is maximal abelian in $\mathfrak{k}_0$.

Lemma 32. *Let $\Gamma_{\mathfrak{k}_0}$ be a maximal abelian subalgebra of $\mathfrak{k}_0$ and Γ_0 the centralizer of $\Gamma_{\mathfrak{k}_0}$ in $\mathfrak{g}_0$. Then Γ_0 is a Cartan subalgebra of $\mathfrak{g}_0$ and $\theta(\Gamma_0) = \Gamma_0$.*

Since $\theta(\Gamma_{\mathfrak{k}_0}) = \Gamma_{\mathfrak{k}_0}$, it is obvious that $\theta(\Gamma_0) = \Gamma_0$. Let $X, Y \in \Gamma_{\mathfrak{p}_0} = \Gamma_0 \cap \mathfrak{p}_0$. Then $Z = [X, Y] \in \Gamma_0 \cap \mathfrak{k}_0 = \Gamma_{\mathfrak{k}_0}$ and $\| Z \|^2 = -B(Z, Z) = B(Y, [X, Z]) = 0$ since $[X, Z] = 0$. This proves that $Z = 0$, and therefore $\Gamma_0 = \Gamma_{\mathfrak{k}_0} + \Gamma_{\mathfrak{p}_0}$ is abelian. Let $\mathfrak{a}_0$ be any Cartan subalgebra of $\mathfrak{g}_0$ containing $\Gamma_{\mathfrak{k}_0}$. Then $\mathfrak{a}_0 \subset \Gamma_0$. But since $\mathfrak{a}_0$ is maximal abelian in $\mathfrak{g}_0$, it follows that $\mathfrak{a}_0 = \Gamma_0$. This proves our assertion.

Corollary. *Any two fundamental Cartan subalgebras of $\mathfrak{g}_0$ are conjugate under G.*

Let Γ_1, Γ_2 be two fundamental Cartan subalgebras of $\mathfrak{g}_0$. By replacing them by conjugate subalgebras, we may assume that $\theta(\Gamma_i) = \Gamma_i$ $(i = 1, 2)$. Then from the Corollary to Lemma 31, $\Gamma_i \cap \mathfrak{k}_0$ is maximal abelian in $\mathfrak{k}_0$. However, since K is compact, any two maximal abelian subalgebras of $\mathfrak{k}_0$ are conjugate under K. Hence $\Gamma_2 \cap \mathfrak{k}_0 = (k\Gamma_1) \cap \mathfrak{k}_0$ for some $k \in K$. But then it follows from Lemma 32 that $\Gamma_2 = k\Gamma_1$.

Lemma 33. *Let Γ_0 be a Cartan subalgebra of $\mathfrak{g}_0$ and Γ its complexification in $\mathfrak{g}$. Then the following two conditions on Γ_0 are equivalent.*

(1) *Γ is not fundamental.*

(2) *There exists a root α* (of $\mathfrak{g}$ with respect to Γ) *which takes only real values on Γ_0.*

Again we may assume that $\theta(\Gamma_0) = \Gamma_0$. Since every root α takes only pure imaginary values on $\Gamma_0 \cap \mathfrak{k}_0$, condition (2) is obviously equivalent to the following:

(3) *There exists a root α which vanishes identically on $\Gamma \cap \mathfrak{k}$.*

Now if Γ_0 is fundamental, Γ is exactly the centralizer of $\Gamma \cap \mathfrak{k}$ in $\mathfrak{g}$ (Lemma 32), and therefore no root can vanish identically on $\Gamma \cap \mathfrak{k}$. This proves that (3) implies (1). Conversely, suppose (3) is false. Then no root can vanish identically on $\Gamma \cap \mathfrak{k}$, and therefore it is obvious that Γ is exactly the centralizer of $\Gamma \cap \mathfrak{k}$ in $\mathfrak{g}$. This proves that $\Gamma_0 \cap \mathfrak{k}_0$ is maximal abelian in $\mathfrak{k}_0$, and so Γ_0 is fundamental. Hence (1) and (3), and therefore also (1) and (2), are equivalent.

We now return to the notation of Section 5. Let Q_+ be the set of those $\alpha \in P$ which take only real values on $\mathfrak{h}_0$. Put $Q' = Q_+ \cup P_-$, and let $W_{Q'}$ be the subgroup of the Weyl group W (of $\mathfrak{g}$ with respect to $\mathfrak{h}$) generated by the Weyl reflexions s_α corresponding to $\alpha \in Q'$.

LEMMA 34. *Suppose* $s \in W_{Q'}$. *Then* $s\mathfrak{h}_0 = \mathfrak{h}_0$ *and*

$$\phi_f(sH) = \epsilon(s)\phi_f(H)$$

for $f \in \mathscr{C}(\mathfrak{g}_0)$ *and* $H \in \mathfrak{h}_0'$.

Let A' be the normalizer of A in G. Then for every $y \in A'$, we get a transformation τ_y of $G^* = G/A$ onto itself given by $\tau_y(x^*) = (xy)^*$ $(x \in G)$. Since A is of finite index in A' (see [2(e), §2]), τ_y^k is the identity for some integer $k \geqq 1$, and from this it follows immediately that the measure dx^* on G^* is invariant under τ_y.

Now from Corollary 2 to Lemma 46 of the Appendix (Section 12) we can choose $y \in G$ such that $yH = sH$ for all $H \in \mathfrak{h}$. Then it is clear that $s\mathfrak{h}_0 = \mathfrak{h}_0$ and $y \in A'$. Therefore if $f \in \mathscr{C}(\mathfrak{g}_0)$,

$$\phi_f(sH) = \pi(sH) \int_{G^*} f(x^*yH)dx^* = \epsilon(s)\pi(H) \int_{G^*} f(x^*H)dx^* = \epsilon(s)\phi_f(H)$$

for $H \in \mathfrak{h}'$.

COROLLARY. *If* $\mathfrak{h}_0$ *is not fundamental, the distribution* T *of Lemma* 26 *is zero.*

We know from Lemma 33 that Q_+ is not empty. Let V_1 denote the closure of $\mathfrak{h}_1$ in $\mathfrak{h}_0$. It follows from Lemma 45 of the Appendix (§12) that we can choose a point $H_0 \in V_1$ and a root $\alpha \in Q_+$ such that $\alpha(H_0) = 0$ while $\beta(H_0) \neq 0$ for any positive root $\beta \neq \alpha$. It is obvious that $tH_0 \in V_1$ for any positive number t. Let s_α denote the Weyl reflexion corresponding to α and for a fixed $f \in \mathscr{C}(\mathfrak{g}_0)$, put

$$\psi_f(H) = \epsilon_+(H)\phi_f(H) \qquad (H \in \mathfrak{h}_0')$$

in the notation of Theorem 3. Since $\mathfrak{h}_\mathfrak{k}$ and $\mathfrak{h}_\mathfrak{p}$ are orthogonal, it is clear where the star denotes the adjoint of a differential operator. But

$$\lambda_X(Z;\partial(\omega))=\omega'(X)\lambda_X(Z) \qquad (Z\in\mathfrak{g}_0).$$

Therefore[11] if $g_i=q_ig$,

$$\omega'(\zeta g)\hat{}_{\alpha_0}=\sum_{1\leqq i\leqq r}(\hat{g}_i)_{b_i*\alpha_0}+(D^*g)\hat{}_{\alpha_c}.$$

Moreover since the b_i are homogenous of degree 2, it is obvious that $b_i=b_i^*\in\mathfrak{B}\mathfrak{g}$ and so $\int\alpha_0(x;b_i^*)\,dx=0$. So we conclude that

$$\omega'(\bar{H}_0)\sigma_{\bar{H}_0}(\zeta g)=\sigma_{\bar{H}_0}(D^*g),$$

and this proves that $D\sigma_{\bar{H}_0}=\omega'(\bar{H}_0)\zeta\sigma_{\bar{H}_0}$.

Define the mapping $f\rightarrow\psi_f$ of $\mathscr{C}(\mathfrak{h}_0)$ into $J(\mathfrak{k}_0)$ as in Lemma 27 of [2(h)] and put $\Phi_{\bar{H}_0}(f)=\sigma_{\bar{H}_0}(\zeta\psi_f)$ $(f\in\mathscr{C}(\mathfrak{h}_0))$. Then $\Phi_{\bar{H}_0}$ is a $\mathscr{C}$-distribution, which, from Theorem 5 of [2(h)], coincides with an analytic function on $\mathfrak{h}_0$. Our first object is to show that $\Phi_{\bar{H}_0}=0$ if $\bar{\mathfrak{h}}_0$ is not conjugate to $\mathfrak{h}_0$ under G. For this we need a few lemmas.

LEMMA 36. *For any* $f\in C_c^\infty(G\times\mathfrak{h}_0')$, *put*

$$\hat{f}(X)=\int_{G\times\mathfrak{h}_0'}\exp\{(-1)^{\frac{1}{2}}B(X,xH)\}f(x,H)\,dx\,dH \qquad (X\in\mathfrak{g}_0),$$

where dH *is the regular Euclidean measure on* $\mathfrak{h}_0'$. *Then* $\hat{f}\in\mathscr{C}(\mathfrak{g}_0)$ *and* $f\rightarrow\hat{f}$ *is a continuous mapping of* $C_c^\infty(G\times\mathfrak{h}_0')$ *into* $\mathscr{C}(\mathfrak{g}_0)$.

Put $G^*=G/A$ as before, and let H_0 be any point in $\mathfrak{h}_0'$. Then we can select (see Section 6) an open neighborhood U of H_0 in $\mathfrak{h}_0'$ such that the mapping $\phi:(x^*,H)\rightarrow x^*H$ of $G^*\times U$ into $\mathfrak{g}_0$ is univalent and regular and, if the Euclidean measure dX on $\mathfrak{g}_0$ is suitably normalized, $dX=|\pi(H)|^2dx^*dH$ $(X=x^*H, x^*\in G^*, H\in U)$. Then $N=\phi(G^*\times U)$ is an open subset of $\mathfrak{g}_0$ and ϕ defines an analytic isomorphism of $G^*\times U$ with N. Therefore, for any $f\in C_c^\infty(G\times U)$, we can define a function $F_f\in C_c^\infty(N)$ by

$$F_f(x^*H)=|\pi(H)|^2\int_A f(xa,H)\,da \qquad (x\in G, H\in U).$$

Here da is the Haar measure on A normalized so that

$$\int_G g(x)\,dx=\int_{G^*}dx^*\int_A g(xa)\,da \qquad (g\in C_c(G)).$$

---

[11] Here $(h)\hat{}_{\alpha}=(\hat{h})_{\alpha}$ for $h\in\mathscr{C}(\mathfrak{k}_0)$ and $\alpha\in C_c^\infty(G)$.

It is now clear that

$$\hat{f}(X') = \int_{\mathfrak{g}_0} \exp\{(-1)^{\frac{1}{2}} B(X', X)\} F_f(X)\, dX \qquad (X' \in \mathfrak{g}_0),$$

and therefore $\hat{f}$ is the Fourier transform of F_f. This proves that $\hat{f} \in \mathcal{C}(\mathfrak{g}_0)$. Moreover, since ϕ is an analytic isomorphism, the mapping $f \rightarrow F_f$ of $C_c^\infty(G \times U)$ into $C_c^\infty(N)$ is obviously continuous, and so the same holds for the mapping $f \rightarrow \hat{f}$ of $C_c^\infty(G \times U)$ into $\mathcal{C}(\mathfrak{g}_0)$. The statement of the lemma now follows from the fact that any compact subset of $\mathfrak{h}_0'$ can be covered by a finite number of sets of the type U.

For a fixed $\bar{H} \in \bar{\mathfrak{h}}_0'$, put

$$T_{\bar{H}}(g) = \bar{\pi}(\bar{H}) \int_{\bar{G}} g(\bar{x}\bar{H})\, d\bar{x} \qquad (g \in \mathcal{C}(\mathfrak{g}_0)).$$

Then from Theorem 3, $T_{\bar{H}}$ is a $\mathcal{C}$-distribution on $\mathfrak{g}_0$. Put $\Phi_f(\bar{H}) = T_{\bar{H}}(\hat{f})$ for $f \in C_c^\infty(G \times \mathfrak{h}_0')$. Then it follows from Lemma 36 that for fixed $\bar{H}$ the mapping $f \rightarrow \Phi_f(\bar{H})$ is a distribution on $G \times \mathfrak{h}_0'$. If $\alpha \in C_c^\infty(G)$ and $\beta \in C_c^\infty(\mathfrak{h}_0')$, we denote by $\alpha \times \beta$ the function $\gamma \in C_c^\infty(G \times \mathfrak{h}_0')$ given by $\gamma(x, H) = \alpha(x)\beta(H)$ $(x \in G, H \in \mathfrak{h}_0')$.

LEMMA 37. *For any $\bar{H} \in \bar{\mathfrak{h}}_0'$, there exists a distribution $\tau_{\bar{H}}'$ on $\mathfrak{h}_0'$ such that*

$$\Phi_{\alpha \times \beta}(\bar{H}) = \int_G \alpha(x)\, dx\, \tau_{\bar{H}}'(\beta)$$

for $\alpha \in C_c^\infty(G)$ and $\beta \in C_c^\infty(\mathfrak{h}_0')$.

It is obvious that for a fixed β, the mapping $\alpha \rightarrow \Phi_{\alpha \times \beta}(\bar{H})$ is a distribution on G which is invariant under left translations. Therefore from Lemma 36 of [2(e)], there exists a constant c_β such that

$$\Phi_{\alpha \times \beta}(\bar{H}) = c_\beta \int_G \alpha(x)\, dx \qquad (\alpha \in C_c^\infty(G)).$$

Select $\alpha_0 \in C_c^\infty(G)$ such that $\int_G \alpha_0(x)\, dx = 1$. Then $c_\beta = \Phi_{\alpha_0 \times \beta}(\bar{H})$. But it is evident that the mapping $\tau_{\bar{H}}' : \beta \rightarrow \Phi_{\alpha_0 \times \beta}(\bar{H})$ $(\beta \in C_c^\infty(\mathfrak{h}_0'))$ is a distribution on $\mathfrak{h}_0'$. Hence

$$\Phi_{\alpha \times \beta}(\bar{H}) = \int_G \alpha(x)\, dx\, \tau_{\bar{H}}'(\beta) \qquad (\alpha \in C_c^\infty(G), \beta \in C_c^\infty(\mathfrak{h}_0')).$$

Put $\tau_{\bar{H}} = \pi \tau_{\bar{H}}'$ $(\bar{H} \in \bar{\mathfrak{h}}_0')$.

LEMMA 38. *For any* $p \in I(\mathfrak{g})$ *and* $\bar{H} \in \mathfrak{h}_0'$,

$$\partial(\bar{p})\tau_{\bar{H}} = p'(\bar{H})\tau_{\bar{H}}$$

where $\bar{p}$ *denotes the restriction of* p *on* $\mathfrak{h}$.

We use the notation of the proof of Lemma 35. It is obvious that

$$\lambda_X(Z;\partial(q)) = q'(X)\lambda_X(Z) \qquad (X, Z \in \mathfrak{g}_0; q \in S(\mathfrak{g})).$$

Select $\alpha \in C_c^\infty(G)$ such that $\int \alpha(x)dx = 1$, and fix $\beta \in C_c^\infty(\mathfrak{h}_0')$. Then if if $p \in I(\mathfrak{g})$, it follows from Lemmas 5 and 8 of [2(h)] that

$$\begin{aligned} p'(X)\lambda_X(xH) &= \lambda_X(xH;\partial(p)) \\ &= \sum_{1\leqq i\leqq N} a_i(H)\Lambda_X(x;b_i:H;\partial(u_i)) + \pi(H)^{-1}\Lambda_X(x:H;\partial(\bar{p})\circ\pi) \end{aligned}$$

for $x \in G, H \in \mathfrak{h}_0'$ and $X \in \mathfrak{g}_0$. Here $u_i \in S(\mathfrak{h})$, $b_i \in \mathfrak{B}\mathfrak{g}$ and the a_i are analytic functions on $\mathfrak{h}_0'$. Hence if $\gamma = \alpha \times \beta$,

$$p'(X)\hat{\gamma}(X) = \sum_{1\leqq i\leqq N}\int \alpha_i(x)\beta_i(H)\lambda_X(xH)dxdH + \int \alpha(x)\beta'(H)\lambda_X(xH)dxdH$$

where $\alpha_i = b_i{}^*\alpha$, $\beta_i = (\partial(u_i))^*(a_i\beta)$ $(1 \leqq i \leqq N)$ and $\beta' = (\pi^{-1}\partial(\bar{p})\circ\pi)^*\beta$. (As usual the star denotes the adjoint of a differential operator). But then

$$\int \alpha_i(x)dx = \int \alpha(x;b_i{}^*)dx = 0$$

and so it follows from Lemma 37 that

$$T_{\bar{H}}(p'\hat{\gamma}) = \tau_{\bar{H}}'(\beta').$$

Moreover $p' \in I(\mathfrak{g})$ and therefore it is obvious that

$$T_{\bar{H}}(p'\gamma) = p'(\bar{H})T_{\bar{H}}(\hat{\gamma}) = p'(\bar{H})\tau_{\bar{H}}'(\beta).$$

This proves that

$$\tau_{\bar{H}}'(\beta') = p'(\bar{H})\tau_{\bar{H}}'(\beta).$$

But $\beta' = (\pi^{-1}\partial(\bar{p})\circ\pi)^*\beta$. Hence if we replace β by $\pi\beta$, we get

$$\tau_{\bar{H}}((\partial(\bar{p}))^*\beta) = p'(\bar{H})\tau_{\bar{H}}(\beta),$$

and so the lemma is proved.

Now normalize the Euclidean measure dY on $\mathfrak{k}_0$ in such a way that

$$\int_{\mathfrak{k}_0} g(Y)dY = \int_{\mathfrak{h}_0} |\pi_-(H)|^2 dH \int_K g(kH)dK \qquad (g \in C_c(\mathfrak{k}_0)).$$

Here $\pi_- = \prod_{\alpha \in P_-} \alpha$ and dk is the Haar measure on K $(\int_K dk = 1)$. It is easily seen that $\zeta(H)|\pi_-(H)|^2 = (-1)^r \pi(H)^2$ $(H \in \mathfrak{h}_0)$, where r is the degree of π. Therefore it follows that if $f \in \mathscr{C}(\mathfrak{h}_0)$ and $X \in \mathfrak{g}_0$, then

$$\int_{\mathfrak{k}_0} \exp\{(-1)^{\frac{1}{2}} B(X,Y)\}\zeta(Y)\psi_f(Y)dY$$
$$= (-1)^r \int_{K \times \mathfrak{h}_0} \exp\{(-1)^{\frac{1}{2}} B(X,kH)\}\pi(H) \sum_{s \in W} \epsilon(s) f(sH)\, dk dH.$$

Now select $\beta \in C_c^\infty(\mathfrak{h}_0')$ and $\alpha \in C_c^\infty(G)$ $(\int \alpha(x)dx = 1)$, and put[12]

$$\alpha_1(x) = \int_K \alpha(xk)dk, \qquad \beta_1 = \pi \sum_{s \in W} \epsilon(s)\beta^s$$

and $\gamma = \alpha_1 \times \beta_1$. Then $T_{\bar{H}}(\hat{\gamma}) = \Phi_{\alpha_1 \times \beta_1}(\bar{H}) = \tau_{\bar{H}}'(\beta_1)$ since $\int \alpha_1(x)dx = 1$. On the other hand, if $g = \zeta\psi_\beta$,

$$\hat{\gamma}(X) = \int \exp\{(-1)^{\frac{1}{2}} B(X, xkH)\}\alpha(x)\beta_1(H)\, dx dk dH$$
$$= (-1)^r \hat{g}_\alpha(X) \qquad\qquad (X \in \mathfrak{g}_0)$$

in the notation of the proof of Lemma 35. Therefore

$$\tau_{\bar{H}}'(\beta_1) = T_{\bar{H}}(\hat{\gamma}) = (-1)^r \sigma_{\bar{H}}(g) = (-1)^r \Phi_{\bar{H}}(\beta),$$

and so we get the following result.

LEMMA 39. *If the Euclidean measure on* $\mathfrak{k}_0$ *is suitably normalized, we have the relation*

$$\Phi_{\bar{H}}(\beta) = (-1)^r \sum_{s \in W} \epsilon(s)\tau_{\bar{H}}(\beta^s)$$

for all $\beta \in C_c^\infty(\mathfrak{h}_0')$ *and* $\bar{H} \in \bar{\mathfrak{h}}_0'$.

COROLLARY 1. $\partial(\bar{p})\Phi_{\bar{H}} = p'(\bar{H})\Phi_{\bar{H}}$ *for* $p \in I(\mathfrak{g})$ *and* $\bar{H} \in \bar{\mathfrak{h}}_0'$.

We know from Lemma 9 of [2(h)] that $\bar{p}$ is invariant under W. Therefore

$$(\partial(\bar{p}))^*\beta^s = ((\partial(\bar{p}))^*\beta)^s \qquad\qquad (s \in W, \beta \in C_c^\infty(\mathfrak{h}_0'))$$

and

$$\Phi_{\bar{H}}((\partial(\bar{p}))^*\beta) = (-1)^r \sum_{s \in W} \epsilon(s)\tau_{\bar{H}}((\partial(\bar{p}))^*\beta^s)$$
$$= (-1)^r p'(\bar{H}) \sum_{s \in W} \epsilon(s)\tau_{\bar{H}}(\beta^s) = p'(\bar{H})\Phi_{\bar{H}}(\beta)$$

---

[12] As usual β^s $(s \in W)$ is defined by $\beta^s(H) = \beta(s^{-1}H)$ $(H \in \mathfrak{h}_0)$.

from Lemma 38. This proves that $\partial(\bar{p})\Phi_{\bar{H}} - p'(\bar{H})\Phi_{\bar{H}}$ is zero on $\mathfrak{h}_0'$. But we have seen that $\Phi_{\bar{H}}$ is an analytic function on $\mathfrak{h}_c$. Therefore $\partial(\bar{p})\Phi_{\bar{H}} = p'(\bar{H})\Phi_{\bar{H}}$ on $\mathfrak{h}_0$.

COROLLARY 2. *Suppose $\mathfrak{h}_0$ is not conjugate to $\bar{\mathfrak{h}}_0$ under G. Then $\Phi_{\bar{H}} = 0$ for every $\bar{H} \in \bar{\mathfrak{h}}_0'$.*

Fix $\bar{H} \in \bar{\mathfrak{h}}_0'$ and consider the $\mathscr{B}$-distribution $\tilde{\Phi}: f \to \Phi_{\bar{H}}(f')$ $(f \in \mathscr{B}(\mathfrak{h}_0))$, where

$$f'(H') = \int_{\mathfrak{h}_0} \exp\{-(-1)^{\frac{1}{2}} B(H', H)\} f(H) \, dH \qquad (H' \in \mathfrak{h}_0).$$

Then it follows from Corollary 1 above that $\bar{p}\tilde{\Phi} = p(\bar{H})\tilde{\Phi}$ $(p \in I(\mathfrak{g}))$, and therefore if H_0 is any point lying in the carrier of $\tilde{\Phi}$, it is obvious that $p(H_0) = p(\bar{H})$ for all $p \in I(\mathfrak{g})$. Let λ be an indeterminate and I the identity mapping of $\mathfrak{g}_0$. Then

$$\det(\lambda I - \operatorname{ad} X) = \sum_{l \leq m \leq n} \lambda^m p_m(X) \qquad (X \in \mathfrak{g}),$$

where $p_m \in I(\mathfrak{g})$. Let $\bar{\mathfrak{h}}$ be the complexification of $\bar{\mathfrak{h}}_0$ in $\mathfrak{g}$ and $\bar{P}$ the set of all positive roots (under some fixed order) of $\mathfrak{g}$ with respect to $\bar{\mathfrak{h}}$. Then

$$\det(\lambda I - \operatorname{ad} H_0) = (-1)^r \lambda^l \prod_{\alpha \in P} (\lambda - \alpha(H_0))^2$$

and similarly,

$$\det(\lambda I - \operatorname{ad} \bar{H}) = (-1)^r \lambda^l \prod_{\bar{\alpha} \in \bar{P}} (\lambda - \bar{\alpha}(\bar{H}))^2.$$

On the other hand, we know from the Corollary to Lemma 32 that $\bar{\mathfrak{h}}_0$ is not a fundamental Cartan subalgebra of $\mathfrak{g}_0$. Therefore from Lemma 33, there exists a root $\bar{\alpha}_0 \in \bar{P}$ which takes only real values on $\bar{\mathfrak{h}}_0$. Then $\bar{\alpha}_0(\bar{H}) \neq 0$ since $\bar{H} \in \bar{\mathfrak{h}}_0'$. On the other hand, every root $\alpha \in P$ takes only pure imaginary values on $\mathfrak{h}_0$ since $\mathfrak{h}_0 \subset \mathfrak{k}_0$. This proves that

$$\det(\lambda I - \operatorname{ad} H_0) \neq \det(\lambda I - \operatorname{ad} \bar{H}),$$

and therefore $p_m(H_0) \neq p_m(\bar{H})$ for some m $(l \leq m \leq n)$. This shows that the carrier of $\tilde{\Phi}$ is empty, and therefore since $\tilde{\Phi}$ is the Fourier transform of $\Phi_{\bar{H}}$ (see Schwartz [6(II)]), we conclude that $\Phi_{\bar{H}} = 0$.

Let us now consider the case when $\bar{\mathfrak{h}}_0 = \mathfrak{h}_0$ and denote by $\Phi(H_0 : H)$ the value of the analytic function Φ_{H_0} at H $(H_0 \in \mathfrak{h}_0', H \in \mathfrak{h}_0)$.

LEMMA 40. *There exists a locally constant function*[13] *c on $\mathfrak{h}_0'$ such that*

$$\Phi(H_0 : H) = c(H_0) \sum_{s \in W} \epsilon(s) \exp\{(-1)^{\frac{1}{2}} B(sH_0, H)\}$$

for $H_0 \in \mathfrak{h}_0'$ and $H \in \mathfrak{h}_0$.

---

[13] This means that c is constant on some neighborhood of every point in $\mathfrak{h}_0'$ and therefore also on each connected component of $\mathfrak{h}_0'$.

Fix $H_0 \in \mathfrak{h}_0'$. Then it follows from Corollary 1 of Lemma 39 and the Corollary to Lemma 13 of [2(h)] that

$$\Phi(H_0 : H) = \sum_{s \in W} c_s \exp\{(-1)^{\frac{1}{2}} B(sH_0, H)\} \qquad (H \in \mathfrak{h}_0),$$

where the c_s are uniquely determined constants. On the other hand, it is obvious from the definition of Φ_{H_0} that $\Phi_{H_0}(\beta^s) = \epsilon(s)\Phi_{H_0}(\beta)$ $(\beta \in \mathscr{C}(\mathfrak{h}_0), s \in W)$. Hence $\Phi(H_0 : sH) = \epsilon(s)\Phi(H_0 : H)$. Therefore, in view of the uniqueness of c_s, we conclude that $\epsilon(s)c_s$ $(s \in W)$ are all equal. This proves that

$$\Phi(H_0 : H) = c(H_0) \sum_{s \in W} \epsilon(s) \exp\{(-1)^{\frac{1}{2}} B(sH_0, H)\} \quad (H_0 \in \mathfrak{h}_0', H \in \mathfrak{h}_0),$$

where c is a function on $\mathfrak{h}_0'$.

Now select $\alpha \in C_c^\infty(G)$ such that $\int \alpha(x)\,dx = 1$, and for $\beta \in C_c^\infty(\mathfrak{h}_0')$, put $\gamma = \alpha \times \pi\beta$. Then $\tau_{H_0}(\beta) = T_{H_0}(\hat{\gamma}) = \phi_{\hat{\gamma}}(H_0)$ in the notations of Lemma 36 and Theorem 3. On the other hand,

$$\Phi_{H_0}(\beta) = (-1)^r \sum_{s \in W} \epsilon(s) \tau_{H_0}(\beta^s)$$

from Lemma 39. Therefore

$$c(H) \sum_{s \in W} \epsilon(s) \bar{\beta}(sH) = (-1)^r \sum_{s \in W} \epsilon(s) \phi_{\hat{\gamma}_s}(H)$$

$(H \in \mathfrak{h}_0', \beta \in C_c^\infty(\mathfrak{h}_0'))$, where $\bar{\beta}$ is the Fourier transform of β and $\gamma_s = \alpha \times \pi\beta^s$. Since $C_c^\infty(\mathfrak{h}_0')$ is dense in $\mathscr{C}(\mathfrak{h}_0)$ under the norm

$$\| \beta_1 \| = \int_{\mathfrak{h}_0} |\beta_1(H)|\, dH \qquad (\beta_1 \in \mathscr{C}(\mathfrak{h}_0)),$$

it follows without difficulty that, for a given $H_0 \in \mathfrak{h}_0'$, we can select $\beta \in C_c^\infty(\mathfrak{h}_0')$ such that $\sum_{s \in W} \epsilon(s) \bar{\beta}(sH_0) \neq 0$. Hence, in view of the fact that $\hat{\gamma}_s \in \mathscr{C}(\mathfrak{g}_0)$ (Lemma 36) and ϕ_g is of class C^∞ on $\mathfrak{h}_0'$ for $g \in \mathscr{C}(\mathfrak{g}_0)$ (Theorem 3), we conclude that c is of class C^∞ on $\mathfrak{h}_0'$. Now suppose $p \in I(\mathfrak{g})$. Then it is evident that

$$\gamma(X ; \partial(p)) = \int \exp\{(-1)^{\frac{1}{2}} B(X, xH)\} \alpha(x) p'(H) \pi(H) \beta(H)\, dx\, dH \quad (X \in \mathfrak{g}_0).$$

Hence if $\beta' = \bar{p}'\beta$ and $\gamma' = \alpha \times \pi\beta'$, we get $\partial(p)\hat{\gamma} = \hat{\gamma}'$, and therefore

$$\tau_{H_0}(\beta') = \phi_{\partial(p)\hat{\gamma}}(H_0) = \phi_{\hat{\gamma}}(H_0 ; \partial(\bar{p}))$$

from Theorem 3. Moreover $(\beta')^s = \bar{p}'\beta^s$ $(s \in W)$ since $\bar{p}'$ is invariant under W. Therefore

$$\Phi_{H_0}(\beta') = (-1)^r \sum_{s \in W} \epsilon(s) \tau_{H_0}((\beta')^s) = (-1)^r \sum_{s \in W} \epsilon(s) \phi_{\hat{\gamma}_s}(H_0; \partial(\bar{p}))$$

$$= \int_{\mathfrak{h}_0} \Phi(H_0; \partial(\bar{p}) : H) \beta(H) \, dH.$$

Since β is an arbitrary element in $C_c^\infty(\mathfrak{h}_0')$, we conclude that

$$\Phi(H_0; \partial(\bar{p}) : H) = p'(H) \Phi(H_0 : H) \qquad (H_0 \in \mathfrak{h}_0', H \in \mathfrak{h}_0).$$

But now it follows from Lemma 23 that c is locally constant.

COROLLARY. *There exists a complex number c_0 such that*

$$\sum_{s \in W} \Phi(sH' : H) = c_0 \sum_{s \in W} \epsilon(s) \exp\{(-1)^{\frac{1}{2}} B(sH', H)\}$$

for all $H' \in \mathfrak{h}_0'$ and $H \in \mathfrak{h}_0$.

Let $\mathfrak{h}_1$ be a connected component of $\mathfrak{h}_0'$. Then (see Lemma 44 of the Appendix, Section 12) $\mathfrak{h}_0' = \bigcup_{s \in W} s\mathfrak{h}_1$, and so it is evident that $c_0 = \sum_{s \in W} c(sH')$ $(H' \in \mathfrak{h}_0')$ is independent of H'. From this our assertion follows immediately.

The main results of this section can now be summarized in the following theorem.

THEOREM 4. *Let $\mathfrak{h}_0$ and $\bar{\mathfrak{h}}_0$ be two Cartan subalgebras of $\mathfrak{g}_0$. We assume that $\mathfrak{h}_0 \subset \mathfrak{k}_0$ and*[14] *$\theta(\bar{\mathfrak{h}}_0) = \bar{\mathfrak{h}}_0$. For any $f \in \mathcal{C}(\mathfrak{h}_0)$, put*

$$\hat{f}(X) = \int_{K \times \mathfrak{h}_0} \exp\{(-1)^{\frac{1}{2}} B(X, kH)\} \pi(H)^2 \sum_{s \in W} f(sH) \, dk \, dH \qquad (X \in \mathfrak{g}_0).$$

Then the integral

$$\phi_{\hat{f}}(\bar{H}) = \bar{\pi}(\bar{H}) \int_{\bar{G}} \hat{f}(\bar{x}\bar{H}) \, d\bar{x}$$

is convergent for $\bar{H} \in \bar{\mathfrak{h}}_0'$. Moreover in case $\bar{\mathfrak{h}}_0$ is not conjugate to $\mathfrak{h}_0$ under G, $\phi_{\hat{f}} = 0$ on $\bar{\mathfrak{h}}_0'$. On the other hand, if $\bar{\mathfrak{h}}_0 = \mathfrak{h}_0$, there exists a complex number c_0 such that

$$\sum_{s \in W} \epsilon(s) \phi_{\hat{f}}(sH') = c_0 \int_{\mathfrak{h}_0} \sum_{s \in W} \epsilon(s) \exp\{(-1)^{\frac{1}{2}} B(H', sH)\} \pi(H) f(H) \, dH$$

for $H' \in \mathfrak{h}_0'$ and $f \in \mathcal{C}(\mathfrak{h}_0)$.

---

[14] In view of the corollary to Lemma 1 of [2(e)], our assumption that $\theta(\bar{\mathfrak{h}}_0) = \bar{\mathfrak{h}}_0$ is obviously unnecessary. We make it here only for convenience.

It is evident that $\phi_{\hat{f}}(\bar{H})=(-1)^r\Phi_{\bar{H}}(\pi f)$ $(f\in\mathcal{B}(\mathfrak{h}_0),\ \bar{H}\in\bar{\mathfrak{h}}_0')$ in our earlier notation. Therefore, from Corollary 2 to Lemma 39, $\phi_{\hat{f}}=0$ if $\bar{\mathfrak{h}}_0$ is not conjugate to $\mathfrak{h}_0$ On the other hand, if $\mathfrak{h}_0=\mathfrak{h}_0$, our assertion follows from the Corollary to Lemma 40. We shall prove in Section 11 that $c_0\neq 0$.

10. Some work of de Rham. Let E be a Euclidean space over R of dimension $n\geqq 3$, and let p,q be two nonnegative integers such that $p+q=n$. Let $(x_1,\cdots,x_n)$ be a Cartesian system of coordinates on E and put $y_i=x_{p+i}$ $(1\leqq i\leqq q)$. We consider the differential operator

$$\square=\frac{\partial^2}{\partial x_1^2}+\cdots+\frac{\partial^2}{\partial x_p^2}-\left(\frac{\partial^2}{\partial y_1^2}+\cdots+\frac{\partial^2}{\partial y_q^2}\right)$$

on E. Let dX denote the Euclidean measure on E so normalized that $dX=dx_1\cdots dx_n$. Then every locally summable function ξ on E defines, as usual, a distribution

$$f\to\int_E f\xi dX \qquad (f\in C_c^\infty(E))$$

which will also be denoted by ξ. Let δ denote the Dirac distribution given by $\delta(f)=f(0)$ and put $u=x_1^2+\cdots+x_p^2-(y_1^2+\cdots+y_q^2)$. Then de Rham has shown[15] that there exists a function ξ on R with the following properties. Put $\Xi(X)=\xi(u(X))$ $(X\in E)$. Then Ξ is a locally summable function on E and

$$\square^{[n/2]}\Xi=\delta$$

in the sense of distribution theory. (Here $[t]$ denotes the largest integer not exceeding $t\in R$). The actual expressions for ξ in the various possible cases are given below in terms of the Heaviside function $Y(t)$ which is 0 or 1 according as $t\leqq 0$ or $t>0$ $(t\in R)$. There are four cases.[16]

(1) If $n\equiv p\equiv 1 \bmod 2$,

$$\xi(t)=(-1)^{(p-1)/2}\{\pi^{\frac{1}{2}(n-2)}4^{n-2}\Gamma((n-2)/2)\}^{-1}Y(t)t^{-\frac{1}{2}}.$$

(2) If $n\equiv q\equiv 1 \bmod 2$,

$$\xi(t)=(-1)^{p/2}\{\pi^{\frac{1}{2}(n-2)}4^{n-2}\Gamma((n-2)/2)\}^{-1}Y(-t)|t|^{-\frac{1}{2}}.$$

(3) If $n\equiv p\equiv 0 \bmod 2$,

$$\xi(t)=(-1)^{(p-2)/2}\{(4\pi)^{n/2}\Gamma(n/2)\}^{-1}\log|t|.$$

---

[15] I am grateful to Professor de Rham for communicating his results to me, which, so far as I know, have not yet been published.

[16] Here Γ stands for the classical Gamma function.

(4) If $p \equiv q \equiv 1 \bmod 2$,

$$\xi(t) = (-1)^{(p-1)/2}\{(4\pi)^{(n-2)/2}\Gamma((n-2)/2)\}^{-1} Y(t).$$

Put $P = x_1^2 + \cdots + x_p^2$, $Q = y_1^2 + \cdots, y_q^2$. Then a simple calculation shows that

$$c = \int_E |\Xi|(1+P)^{-m}(1+Q)^{-m}\,dX < \infty$$

if m is a sufficiently large positive integer. Hence

$$\int |\Xi f|\,dX \leqq c \sup_{X \in E} |(1+P(X))^m(1+Q(X))^m f(X)|$$

for $f \in \mathscr{B}(E)$. This proves that Ξ can be regarded as a $\mathscr{B}$-distribution. Therefore, since $\square$ is obviously self-adjoint, we get

$$f(0) = \int_E \Xi \square^{[n/2]} f\,dX$$

for any $f \in \mathscr{B}(E)$.

11. An application of the above formula. Let ω be the Casimir polynomial of $\mathfrak{g}$ and put $\square = \partial(\omega)$. Then it is clear from the results of Section 10 that there exists a function ξ on R such that $\Xi(X) = \xi(\omega(X))$ $(X \in \mathfrak{g}_0)$ is a locally summable function on $\mathfrak{g}_0$ and

$$f(0) = \int_{\mathfrak{g}_0} \Xi \partial(\omega^m) f\,dX \qquad (f \in \mathscr{B}(\mathfrak{g}_0)).$$

Here $m = [n/2]$, $n = \dim_R \mathfrak{g}_0$ and dX is the regular Euclidean measure on $\mathfrak{g}_0$. (Since $\mathfrak{g}_0$ is semisimple it is obvious that $n \geqq 3$). We shall apply this formula to prove that the constant c_0 of Theorem 4 is not zero. So let us assume that $\mathfrak{h}_0$ is a Cartan subalgebra of $\mathfrak{g}_0$ which is contained in $\mathfrak{k}_0$. Select a finite set of Cartan subalgebras $\mathfrak{h}_0 = \mathfrak{h}_1, \mathfrak{h}_2, \cdots, \mathfrak{h}_N$ of $\mathfrak{g}_0$ such that $\theta(\mathfrak{h}_i) = \mathfrak{h}_i$ $(1 \leqq i \leqq N)$ and every Cartan subalgebra of $\mathfrak{g}_0$ is conjugate under G to $\mathfrak{h}_i$ for exactly one i $(1 \leqq i \leqq N)$. We know (see the Corollary to Lemma 2 of [2(e)]) that this is possible. Let $(\mathfrak{h}_i)_c$ denote the complexification of $\mathfrak{h}_i$ in $\mathfrak{g}$ and P_i the set of all positive roots of $\mathfrak{g}$ with respect to $(\mathfrak{h}_i)_c$ under some fixed order. (We assume that $P_1 = P$.) Put $\pi_i = \prod_{\alpha \in P_i} \alpha$ and let W_i denote the Weyl group of $\mathfrak{g}$ with respect to $(\mathfrak{h}_i)_c$. Consider the Cartan subgroup A_i of G corresponding to $\mathfrak{h}_i$ and the normalizer A_i' of A_i

in G. Then[17] the factor group $W_i' = A_i'/A_i$ can be regarded as a subgroup of W_i. Put $G_i^* = G/A_i$, and define x^*H $(x^* \in G_i^*, H \in \mathfrak{h}_i)$ in the usual way. We have seen in Section 8 that W_i' operates on G_i^* on the right. Let $\mathfrak{g}_0'$ be the set of regular elements of $\mathfrak{g}_0$, and put $\mathfrak{h}_i' = \mathfrak{g}_0' \cap \mathfrak{h}_i$. Consider the mapping $\psi_i \colon (x^*, H) \rightarrow x^*H$ of $G_i^* \times \mathfrak{h}_i'$ into $\mathfrak{g}_0'$, and put $\psi_i(G_i^* \times \mathfrak{h}_i') = \mathfrak{g}_i$. Then ψ_i is everywhere regular on $G_i^* \times \mathfrak{h}_i'$, and therefore $\mathfrak{g}_i$ is open in $\mathfrak{g}_0$ and if w_i' is the order of W_i', any element x^*H $(x^* \in G_i^*, H \in \mathfrak{h}_i')$ of $\mathfrak{g}_i$ has exactly w_i' distinct pre-images under ψ_i, namely, $(x^*s, s^{-1}H_i)$ $(s \in W')$. Let d_iH denote the regular Euclidean measure on $\mathfrak{h}_i$. Then the invariant measure d_ix^* on G_i^* can be so normalized that

$$\int_{\mathfrak{g}_i} g(X)\,dX = \int_{G_i^* \times \mathfrak{h}_i'} |\pi_i(H)|^2 g(x^*H)\, d_ix^* d_iH \qquad (g \in C_c(\mathfrak{g}_i)).$$

Since no two among $\mathfrak{h}_1, \cdots, \mathfrak{h}_N$ are conjugate under G, it is clear that the sets $\mathfrak{g}_1, \cdots, \mathfrak{g}_N$ are disjoint. Moreover, if X is any regular element in $\mathfrak{g}_0$, its centralizer $\mathfrak{h}_X$ (in $\mathfrak{g}_0$) in a Cartan subalgebra of $\mathfrak{g}_0$ which must be conjugate to some $\mathfrak{h}_i$. This proves that $\mathfrak{g}_0' = \bigcup_{1 \leqq i \leqq N} \mathfrak{g}_i$, and therefore

$$\int_{\mathfrak{g}_0} g(X)\,dX = \int_{\mathfrak{g}_0'} g(X)\,dX = \sum_{1 \leqq i \leqq N} \int_{G_i^* \times \mathfrak{h}_i'} |\pi_i(H)|^2 g(x^*H)\, d_ix^* d_iH \qquad (g \in C_c(\mathfrak{g}_0)).$$

Now for any $f \in \mathscr{E}(\mathfrak{g}_0)$, put

$$\phi_f^{(i)}(H) = \pi_i(H) \int_{G_i^*} f(x^*H)\, d_ix^* \qquad (H \in \mathfrak{h}_i').$$

From Theorem 3, we know that this integral is convergent, and it follows from Fubini's Theorem that[18]

$$\int_{\mathfrak{g}_0} \Xi f\, dX = \sum_{1 \leqq i \leqq N} \int_{\mathfrak{h}_i'} (\operatorname{conj} \pi_i(H))\, \Xi(H) \phi_f^{(i)}(H)\, d_iH \qquad (f \in \mathscr{E}(\mathfrak{g}_0)).$$

Now put $G_1^* = G^*$, $d_1x^* = dx^*$, $d_1H = dH$ and $\pi_1 = \pi$ as before and select two real-valued nonnegative functions α_0 and β_0 in $C_c^\infty(G^*)$ and $C_c^\infty(\mathfrak{h}_0')$, respectively, such that

$$\int_{G^*} \alpha_0(x^*)\,dx^* = \int_{\mathfrak{h}_0} |\pi(H)|^2 \beta_0(H)\,dH = 1.$$

---

[17] All the facts stated here have already been seen in Sections 6 and 8.

[18] We denote the complex conjugate of c by conj c $(c \in C)$.

Put $\alpha(x^*) = (w_1')^{-1} \sum_{s \in W_1'} \alpha_0(x^*s)$ and[12] $\beta = w^{-1} \sum_{s \in W} \beta_0^s$, where $W = W_1$ and w is the order of W. We have seen in Section 8 that the measure dx^* is invariant under the transformation $x^* \rightarrow x^*s$ of G^* for any fixed $s \in W_1'$. Hence

$$\int_{G^*} \alpha(x^*)\, dx^* = \int_{\mathfrak{h}_0} |\pi(H)|^2 \beta(H)\, dH = 1,$$

and it is obvious that there exists a function $F \in C_c^\infty(\mathfrak{g}_1)$ such that $F(x^*H) = \alpha(x^*)\beta(H)$ $(x^* \in G^*, H \in \mathfrak{h}_0')$. Consider its Fourier transform $\bar{F}$ and, for any fixed i $(1 \leqq i \leqq N)$, put $\mathfrak{h}_i = \bar{\mathfrak{h}}_0$. Then since

$$\begin{aligned} \bar{F}(X') &= \int \exp\{(-1)^{\frac{1}{2}} B(X', X)\} F(X)\, dX \\ &= \int_{G^* \times \mathfrak{h}_0'} \exp\{(-1)^{\frac{1}{2}} B(X', x^*H)\} \alpha(x^*) |\pi(H)|^2 \beta(H)\, dx^* dH, \end{aligned}$$

it is obvious from Lemma 37 that

$$\phi_{\bar{F}}^{(i)}(\bar{H}) = (-1)^r \tau_{\bar{H}}(\pi\beta) \qquad (\bar{H} \in \bar{\mathfrak{h}}_0')$$

in the notation of Section 9. Moreover $(\pi\beta)^s = \epsilon(s)\pi\beta$ $(s \in W)$, and so it follows from Lemma 39 that

$$\tau_{\bar{H}}(\pi\beta) = w^{-1}(-1)^r \Phi_{\bar{H}}(\pi\beta).$$

Therefore if $i \neq 1$, $\phi_{\bar{F}}^{(i)} = 0$ from Corollary 2 to Lemma 39. Now suppose $i = 1$. Then if we write $\phi_{\bar{F}}$ instead of $\phi_{\bar{F}}^{(1)}$, we find from the Corollary to Lemma 40 that

$$\sum_{s \in W} \epsilon(s) \phi_{\bar{F}}(sH') = c_0 \int_{\mathfrak{h}_0} \exp\{(-1)^{\frac{1}{2}} B(H', H)\} \pi(H) \beta(H)\, dH \qquad (H' \in \mathfrak{h}_0')$$

since $(\pi\beta)^s = \epsilon(s)\pi\beta$ $(s \in W)$. On the other hand, $\bar{F} \in \mathscr{C}(\mathfrak{g}_0)$, and therefore

$$\bar{F}(0) = \int_{\mathfrak{g}_0} \Xi \partial(\omega^m) \bar{F}\, dX = \sum_{1 \leqq i \leqq N} \int_{\mathfrak{h}_0'} (\operatorname{conj} \pi_i(H)) \phi_{F_m}^{(i)}(H) \Xi(H)\, dH,$$

where $F_m = \partial(\omega^m)\bar{F}$. But from Theorem 3,

$$\phi_{F_m}^{(i)} = \partial(\omega_i^m) \phi_{\bar{F}}^{(i)}$$

where ω_i is the restriction of ω on $\mathfrak{h}_i$. Therefore $\phi_{F_m}^{(i)} = 0$ if $i \neq 1$, and hence

$$\bar{F}(0) = (-1)^r \int_{\mathfrak{h}_0'} \pi(H) \phi_{\bar{F}}(H; \partial(\bar{\omega}^m)) \Xi(H)\, dH,$$

where $\bar{\varpi} = \omega_1$. But since $\Xi(H) = \xi(\omega(H))$ $(H \in \mathfrak{h}_0')$ and $\bar{\varpi}^s = \bar{\varpi}$ $(s \in W)$, it is obvious that $\Xi(sH) = \Xi(H)$. Moreover, $\pi^s = \epsilon(s)\pi$, and so we conclude that

$$\bar{F}(0) = (-1)^r w^{-1} \int_{\mathfrak{h}_0'} \pi(H) \phi'(H; \partial(\bar{\varpi}^m)) \Xi(H) \, dH,$$

where $\phi'(H) = \sum_{s \in W} \epsilon(s) \phi_{\bar{F}}(sH)$ $(H \in \mathfrak{h}_0')$. On the other hand,

$$\bar{F}(0) = \int_{\mathfrak{g}_0} F(X) \, dX = \int_{G^* \times \mathfrak{h}_0'} F(x^* H) \, |\pi(H)|^2 \, dx^* dH$$
$$= \int \alpha(x^*) \, dx^* \int \beta(H) \, |\pi(H)|^2 \, dH = 1.$$

Therefore ϕ' cannot be identically zero on $\mathfrak{h}_0'$, and this proves that $c_0 \neq 0$.

LEMMA 41. *Suppose $\mathfrak{t}_0$ is a Cartan subalgebra of $\mathfrak{g}_0$ which is contained in $\mathfrak{k}_0$. Let $\mathfrak{h}_{(i)}$ $(1 \leqq i \leqq q)$ be all the distinct connected components of $\mathfrak{h}_0' = \mathfrak{h}_0 \cap \mathfrak{g}_0'$. Then there exists a function $g \in \mathcal{C}(\mathfrak{g}_0)$ such that*

$$\sum_{1 \leqq i \leqq q} \lim_{\mathfrak{h}_{(i)}} \phi_g(0; \partial(\pi)) \neq 0$$

in the notation of Section 7. Moreover the constant c_0 of Theorem 4 is not zero.

Put $g = \bar{F}$. Then since $\pi^s = \epsilon(s)\pi$ $(s \in W)$, it is clear that

$$\phi'(H'; \partial(\pi)) = \sum_{s \in W} \phi_g(sH'; \partial(\pi))$$
$$= c_0 (-1)^{r/2} \int_{\mathfrak{h}_0} \exp\{(-1)^{\frac{1}{2}} B(H', H)\} \pi(H)^2 \beta(H) \, dH \qquad (H' \in \mathfrak{h}_0'),$$

and therefore

$$\lim_{H' \to 0} \sum_{s \in W} \phi_g(sH'; \partial(\pi)) = c_0 (-1)^{r/2} \int_{\mathfrak{h}_0} \pi(H)^2 \beta(H) \, dH = c_0 (-1)^{r/2} \neq 0.$$

Since every $s \in W$ permutes $\mathfrak{h}_{(1)}, \cdots, \mathfrak{h}_{(q)}$ among themselves, the statement of the lemma is now obvious.

12. Appendix.

LEMMA 42. *Let U be an open convex subset of a real Euclidean space E of dimension l, and let $\sigma_1, \cdots, \sigma_N$ be a finite number of vector subspaces of E of dimension $\leqq l - 2$. Let U' denote the complement in U of the set $U \cap (\bigcup_{1 \leqq i \leqq N} \sigma_i)$. Then if X_1, X_2 are any two points in U', we can select*

$X_2' \in U'$ arbitrarily near X_2 such that the straight line-segment joining X_1 and X_2' lies entirely in U'.

By replacing σ_i by a larger linear subspace, if necessary, we may clearly assume that $\dim \sigma_i = l - 2$ $(1 \leqq i \leqq N)$. For each i, select two linear functions α_i, β_i on E such that σ_i is exactly the set of those $X \in E$ where $\alpha_i(X) = \beta_i(X) = 0$. Obviously, α_i and β_i are linearly independent for every i. Let E' denote the complement of $\bigcup_{1 \leqq i \leqq N} \sigma_i$ in E. If Y_1, Y_2 are two points in E', it is evident that the line-segment joining Y_1, Y_2 cannot meet σ_i unless $\{\alpha_i(Y_1)/\beta_i(Y_1)\} = \{\alpha_i(Y_2)/\beta_i(Y_2)\}$. Now suppose X_1, X_2 are two points in U' and Σ is the set of those i $(1 \leqq i \leqq N)$ for which $\{\alpha_i(X_1)/\beta_i(X_1)\} = \{\alpha_i(X_2)/\beta_i(X_2)\}$. For the proof of the lemma, we may obviously assume that Σ is not empty. Then since α_j, β_j are linearly independent for every j, we can select $X \in E$ such that

$$\alpha_i(X)\beta_i(X_1) - \beta_i(X)\alpha_i(X_1) \neq 0$$

for all $i \in \Sigma$. Then if ϵ is a sufficiently small positive number and $X_2' = X_2 + \epsilon X$, it is clear that $X_2' \in U'$ and

$$\alpha_j(X_2')\beta_j(X_1) - \beta_j(X_2')\alpha_j(X_1) \neq 0 \qquad (1 \leqq j \leqq N).$$

This proves that the line-segment joining X_1 and X_2' lies in $U \cap E' = U'$.

COROLLARY. *U' is connected.*

Now we use the notation of Section 6. Define $\mathfrak{h}_0'$ and $\mathfrak{h}_1$ as in Lemma 24 and let Q be the set of those roots $\alpha \in P$ for which α^2 takes only real values on $\mathfrak{h}_0$. Since all roots take only real values on $(-1)^{\frac{1}{2}}\mathfrak{h}_{\mathfrak{k}_0} + \mathfrak{h}_{\mathfrak{p}_0}$, it is obvious that a positive root lies in Q if and only if it vanishes identically either on $\mathfrak{h}_{\mathfrak{k}_0}$ or on $\mathfrak{h}_{\mathfrak{p}_0}$. Let P' denote the complement of Q in P, and, for any $\alpha \in P$, let σ_α denote the set of those $H \in \mathfrak{h}_0$ where $\alpha(H) = 0$. Then σ_α is a linear subspace of $\mathfrak{h}_0$, and if $l = \dim_R \mathfrak{h}_0$, it is clear that $\dim_R \sigma_\alpha = l - 1$ or $l - 2$ according as α lies in Q or P'.

For any $\alpha \in Q$, define $\alpha^* = \alpha$ or $(-1)^{\frac{1}{2}}\alpha$ according as α takes only real or only pure imaginary values on $\mathfrak{h}_0$. Then since $\mathfrak{h}_1$ is connected, α^* must keep constant sign on $\mathfrak{h}_1$. Put $\alpha' = \epsilon_\alpha \alpha^*$, where $\epsilon_\alpha = 1$ or -1 according as α^* is positive or negative on $\mathfrak{h}_1$. Let $\mathfrak{h}_2$ be the set of all $H \in \mathfrak{h}_0$ where $\alpha'(H) > 0$ $(\alpha \in Q)$. Clearly, $\mathfrak{h}_2$ is an open convex subset of $\mathfrak{h}_0$ and $\mathfrak{h}_2 \cap \mathfrak{h}_0'$ is the complement in $\mathfrak{h}_2$ of the set $\mathfrak{h}_2 \cap (\bigcup_{\alpha \in P'} \sigma_\alpha)$. Therefore it follows from the Corollary of Lemma 42 that $\mathfrak{h}_2 \cap \mathfrak{h}_0'$ is connected. On the other hand, it is obvious that $\mathfrak{h}_2 \cap \mathfrak{h}_0' \supset \mathfrak{h}_1$. Therefore, since $\mathfrak{h}_1$ is a maximal connected subset of $\mathfrak{h}_0'$, we conclude that $\mathfrak{h}_1 = \mathfrak{h}_2 \cap \mathfrak{h}_0'$. So the following result is an immediate consequence of Lemma 42.

LEMMA 43. *If H_1, H_2 are any two points in $\mathfrak{h}_1$, we can select $H_2' \in \mathfrak{h}_1$ arbitrarily near H_2 such that the straight line-segment joining H_1 and H_2' lies entirely in $\mathfrak{h}_1$.*

Remark. Let V_1 be the closure of $\mathfrak{h}_1$ in $\mathfrak{h}_0$. Since $\mathfrak{h}_1 = \mathfrak{h}_2 \cap \mathfrak{h}_0'$ is dense in $\mathfrak{h}_2$, it is obvious that V_1 is the set of those points $H \in \mathfrak{h}_0$ where $\alpha'(H) \geqq 0$ $(\alpha \in Q)$. Moreover, $V_1 \cap \mathfrak{h}_0' = \mathfrak{h}_2 \cap \mathfrak{h}_0' = \mathfrak{h}_1$. We shall need these facts a little later.

For a linear function λ on $\mathfrak{h}$ and $s \in W$, define the linear function $s\lambda$ by $(s\lambda)(H) = \lambda(s^{-1}H)$ $(H \in \mathfrak{h})$. Then if α is a root, the same holds for $s\alpha$. Let W_R be the subgroup consisting of those elements in W which map $\mathfrak{h}_0$ onto itself. Then if α^2 is real on $\mathfrak{h}_0$, the same obviously holds for $(s\alpha)^2$ $(s \in W_R)$. This means that s permutes $\{\sigma_\alpha\}_{\alpha \in Q}$ and $\{\sigma_\alpha\}_{\alpha \in P'}$ separately among themselves. Let s_α denote the Weyl reflexion corresponding to any root α. Then $s_\alpha H = H - 2\{\alpha(H)/\alpha(H_\alpha)\}H_\alpha$ $(H \in \mathfrak{h})$, where H_α is the element in $\mathfrak{h}$ determined by the condition $B(H, H_\alpha) = \alpha(H)$ $(H \in \mathfrak{h})$. If $\alpha \in Q$, it is clear that $\alpha(H)H_\alpha \in \mathfrak{h}_0$ for $H \in \mathfrak{h}_0$, and therefore $s_\alpha \in W_R$. Let W_Q be the subgroup of W generated by s_α $(\alpha \in Q)$. Then $W_Q \subset W_R$.

LEMMA 44. $\mathfrak{h}_0' = \bigcup_{s \in W_Q} s\mathfrak{h}_1$.

Let U be the complement in $\mathfrak{h}_0$ of the union of $\sigma_\alpha \cap \sigma_\beta$ $(\alpha, \beta \in P, \alpha \neq \beta)$. Since every root takes only real values on $\mathfrak{h}_{\mathfrak{p}_0} + (-1)^{\frac{1}{2}}\mathfrak{h}_{\mathfrak{k}_0}$, it is obvious that[18] $\alpha(\theta(H)) = -\operatorname{conj} \alpha(H)$ $(H \in \mathfrak{h}_0, \alpha \in P)$. Therefore[19] $\alpha = \pm \theta\alpha$ if and only if $\alpha \in Q$. Hence it follows from the definition of U that no root in P' can vanish anywhere on U. Moreover, it is obvious that $sU = U$ $(s \in W_R)$, and from the Corollary to Lemma 42, U is connected. Let V_1 denote the closure of $\mathfrak{h}_1$ in $\mathfrak{h}_0$, and put $V = \bigcup_{s \in W_Q} sV_1$. We shall first prove that $V = \mathfrak{h}_0$.

Since U is connected and dense in $\mathfrak{h}_0$, it would be enough to show that $V \cap U$ is open. But $V \cap U = \bigcup_{s \in W_Q} s(V_1 \cap U)$. Therefore it would be sufficient to prove that any point $H_0 \in V_1 \cap U$, lies in the interior of $V \cap U$.

---

[19] For any linear function λ on $\mathfrak{h}$, $\theta\lambda$ denotes the function $H \to \lambda(\theta(H))$ $(H \in \mathfrak{h})$.

Since $\mathfrak{h}_1 \subset V \cap U$ and $\mathfrak{h}_1$ is open, we may suppose that $H_0 \notin \mathfrak{h}_1$. Then, in view of the definition of U, there is exactly one root $\alpha_0 \in P$ such that $H_0 \in \sigma_{\alpha_0}$ and moreover $\alpha_0 \in Q$. Therefore $\dim \sigma_{\alpha_0} = l - 1$ and s_{α_0} is the reflexion in the hyperplane σ_{α_0}. Select a positive number ϵ, and let N be the set of those points $H \in \mathfrak{h}_0$ where $\alpha_0'(H) \geqq 0$ and $\| H - H_0 \| \leqq \epsilon$. Then if ϵ is sufficiently small, it is clear that $\alpha'(H) \geqq \frac{1}{2}\alpha'(H_0)$ for any $H \in N$ and α in Q. Therefore $N \subset V_1$ (see the remark after Lemma 43). But it is obvious that $N \cup s_{\alpha_0}N$ consists of all points $H \in \mathfrak{h}_0$ for which $\| H - H_0 \| \leqq \epsilon$, and therefore, since U is open, H_0 lies in the interior of $V \quad U$. This proves that $V = \mathfrak{h}_0$.

Now we have seen above that $V_1 \cap \mathfrak{h}_0' = \mathfrak{h}_1$. Therefore

$$\mathfrak{h}_0' = V \quad \mathfrak{h}_0' = \bigcup_{s \in W_Q} s(V_1 \cap \mathfrak{h}_0') = \bigcup_{s \in W_Q} s\mathfrak{h}_1.$$

Thus the lemma is proved.

Let Q_+ be the set of those roots $\alpha \in Q$ which take only real values on $\mathfrak{h}_0$. It is obvious that a positive root β lies in Q_+ if and only if $H_\beta \in \mathfrak{h}_{\mathfrak{p}_0}$. Hence $Q_+ \subset P_+$ and $Q = Q_+ \cup P_0 \cup P_-$ in the notation of Section 5.

LEMMA 45. *If Q_+ is not empty, there exists a root $\alpha \in Q_+$ such that $V_1 \quad U \cap \sigma_\alpha$ is not empty.*

For otherwise suppose $V_1 \cap U \cap \sigma_\alpha = \emptyset$ for every $\alpha \in Q_+$. Let W_1 be the subgroup of W_Q generated by s_β for $\beta \in P_0 \cup P_-$. Then if we use the notation of the proof of Lemma 44, it is clear that $H_0 \in V_1 \cap U \cap \sigma_{\alpha_0}$ and therefore $\alpha_0 \in P_0 \cup P_-$. Hence it follows immediately that $\bigcup_{s \in W_1} s(V_1 \cap U)$ is open, and therefore $\mathfrak{h}_0 = \bigcup_{s \in W_1} sV_1$ and $\mathfrak{h}_0' = \bigcup_{s \in W_1} s\mathfrak{h}_1$. Now select a root $\alpha \in Q_+$. Then α keeps constant sign on $\mathfrak{h}_1$. Moreover since $\mathfrak{h}_\mathfrak{p}$ and $\mathfrak{h}_\mathfrak{k}$ are orthogonal, it is obvious that $s\alpha = \alpha$ for all $s \in W_1$. Hence α keeps constant sign on $\mathfrak{h}_0' = \bigcup_{s \in W_1} s\mathfrak{h}_1$. As this is evidently false, our assertion follows.

LEMMA 46. *For any $\alpha \in P$, we can select X_α, $X_{-\alpha}$ in such a way that $\bar\theta(X_\alpha) = -X_{-\alpha}$ and $[X_\alpha, X_{-\alpha}] = \{2/\alpha(H_\alpha)\}H_\alpha$. Moreover, if $\alpha \in Q_+$, we can assume that $X_\alpha, X_{-\alpha} \in \mathfrak{g}_0$.*

Since $\operatorname{conj} \alpha(H) = -\alpha(\theta(H))$ $(H \in \mathfrak{h}_0)$, it follows that $[H, \bar\theta(X_\alpha)] = -\alpha(H)\bar\theta(X_\alpha)$ $(H \in \mathfrak{h}_0)$, and therefore we can assume that $X_{-\alpha} = -\bar\theta(X_\alpha)$.

Then $B(X_\alpha, X_{-\alpha}) = -B(X_\alpha, \bar{\theta}(X_\alpha)) = \| X_\alpha \|^2$. Now normalize X_α in such a way that $\| X_\alpha |^2 = 2/\alpha(H_\alpha)$. Then if $H \in \mathfrak{h}$,

$$B([X_\alpha, X_{-\alpha}], H) = B(X_{-\alpha}, [H, X_\alpha]) = \alpha(H) B(X_{-\alpha}, X_\alpha) = \{2/\alpha(H_\alpha)\}\alpha(H),$$

and this shows that $[X_\alpha, X_{-\alpha}] = \{2/\alpha(H_\alpha)\}H_\alpha$. Now suppose $\alpha \in Q_+$. Then if ζ denotes the conjugation of $\mathfrak{g}$ with respect to $\mathfrak{g}_0$, it is clear that $[H, \zeta(X_\alpha)] = \alpha(H)\zeta(X_\alpha)$ $(H \in \mathfrak{h}_0)$. Moreover $\| \zeta(X) \| = \| X \|$ for any $X \in \mathfrak{g}$. Hence $\zeta(X_\alpha) = c^2 X_\alpha$, where c is a unimodular complex number. Therefore, replacing X_α by cX_α, we can assume that $\zeta(X_\alpha) = X_\alpha$ without disturbing the value of $\| X_\alpha \|$. Then $X_\alpha \in \mathfrak{g}_0$ and $X_{-\alpha} = -\bar{\theta}(X_\alpha) = -\theta(X_\alpha)$ is also in $\mathfrak{g}_0$.

COROLLARY 1. *For a fixed $\alpha \in P$, select $X_\alpha, X_{-\alpha}$ according to the above lemma and put $\mathfrak{l} = CH_\alpha + CX_\alpha + CX_{-\alpha}$. Then*

$$\mathfrak{l}_0 = \mathfrak{l} \cap \mathfrak{g}_0 = \begin{cases} RH_\alpha + RX_\alpha + RX_{-\alpha} \text{ if } \alpha \in Q_+, \\ R(-1)^{\frac{1}{2}} H_\alpha + R(-1)^{\frac{1}{2}}(X_\alpha - X_{-\alpha}) + R(X_\alpha + X_{-\alpha}) \text{ if } \alpha \in P_0, \\ R(-1)^{\frac{1}{2}} H_\alpha + R(X_\alpha - X_{-\alpha}) + R(-1)^{\frac{1}{2}}(X_\alpha + X_{-\alpha}) \text{ if } \alpha \in P_-. \end{cases}$$

If $\alpha \in Q_+$, our assertion is obvious. Now suppose $\alpha \in P_0$. Then $X_\alpha \in \mathfrak{p}$, and therefore

$$X_{-\alpha} = -\bar{\theta}(X_\alpha) = \zeta(X_\alpha).$$

Therefore $X_\alpha + X_{-\alpha}$ and $(-1)^{\frac{1}{2}}(X_\alpha - X_{-\alpha})$ are in $\mathfrak{l}_0$ in this case. Similarly, $X_\alpha \in \mathfrak{k}$ and $X_{-\alpha} = -\bar{\theta}(X_\alpha) = -\zeta(X_\alpha)$ if $\alpha \in P_-$. Therefore $X_\alpha - X_{-\alpha}$ and $(-1)^{\frac{1}{2}}(X_\alpha + X_{-\alpha})$ are in $\mathfrak{l}_0$ in this case. Moreover, it is obvious that $\dim_R \mathfrak{l}_0 \leq \dim_C \mathfrak{l} \leq 3$, and so the above statements follow.

Put $H' = 2\alpha(H_\alpha)^{-1}H_\alpha$, $X' = X_\alpha$, $Y' = X_{-\alpha}$. Then $[H', X'] = 2X'$, $[H', Y'] = -2Y'$, $[X', Y'] = H'$, and a simple calculation shows that $\exp(\frac{\pi}{2}\operatorname{ad}(X' - Y'))H' = -H'$. On the other hand, it is obvious that $\exp(\frac{\pi}{2}\operatorname{ad}(X' - Y'))H = H$ if $\alpha(H) = 0$ $(H \in \mathfrak{h})$. Therefore

$$\exp(\tfrac{\pi}{2}\operatorname{ad}(X' - Y'))H = s_\alpha H \qquad (H \in \mathfrak{h}).$$

COROLLARY 2. *If $\alpha \in Q_+ \cup P_-$ there exists an element $x \in K$ such that $xH = s_\alpha H$ for all $H \in \mathfrak{h}$.*

This follows from the fact that $X' - Y' \in \mathfrak{k}_0$ if $\alpha \in Q_+ \cup P_-$.

INSTITUTE FOR ADVANCED STUDY,
COLUMBIA UNIVERSITY.

REFERENCES.

[1] I. M. Gelfand and M. I. Graev, *Doklady Akad. Nauk. SSSR N. S.*, vol. 92 (1953), pp. 461-464.

[2] Harish-Chandra, (a) *Ann. of Math.*, vol. 51 (1950), pp. 299-330.
(b) *Trans. Amer. Math. Soc.*, vol. 70 (1951), pp. 28-96.
(c) " " " " vol. 75 (1953), pp. 185-243.
(d) " " " " vol. 76 (1954), pp. 485-528.
(e) " " " " vol. 83 (1956), pp. 98-163.
(f) *Amer. Jour. Math.*, vol. 77 (1955), pp. 743-777.
(g) " " " vol. 78 (1956), pp. 564-628.
(h) " " " vol. 79 (1957), pp. 87-120.
(i) *Proc. Nat. Acad. Sci. U.S.A.*, vol. 42 (1956), pp. 252-253.
(j) " " " " " vol. 42 (1956), pp. 538-540.

[3] K. Iwasawa, *Ann. of Math.*, vol. 50 (1949), pp. 507-557.

[4] J. L. Koszul, *Bull. Soc. Math. France*, vol. 78 (1950), pp. 65-127.

[5] G. D. Mostow, *Bull. Amer. Math. Soc.*, vol. 55 (1949), pp. 969-980.

[6] L. Schwartz, *Théorie des distributions*, I (1950), II (1951), Paris, Hermann.

[7] A. Weil, *L'integration dans les groupes topologiques et ses applications*, Paris, Hermann, 1940.

[8] H. Weyl, *The structure and representations of continuous groups*, Princeton, The Institute for Advanced Study, 1935.

RESTRICTED BASES.*

By JOHN B. KELLY.

---

1. **Introduction.** A set of non-negative integers is called a basis of order h if every positive integer can be expressed as a sum of h elements of the set and if h is the smallest number for which this is true. A set of non-negative integers is an asymptotic basis of order h if every sufficiently large integer can be expressed as a sum of h or fewer elements of the set and if h is the smallest number for which this is true. Finally, we shall call a set of non-negative integers a restricted basis of order k if every sufficiently large positive integer can be expressed as a sum of k or fewer elements of the set *without repetitions* and if k is the smallest number for which this is true.

The set of squares is, according to Lagrange's theorem, a basis of order 4, and, according to Pall's theorem [1], a restricted basis of order 5. One may conjecture that this example is typical of the general situation; i.e., that every basis or every asymptotic basis is a restricted basis. However, a simple counter-example due to P. T. Bateman shows that this is not the case: If $h > 2$, the set consisting of 1 and all non-negative multiples of h is a basis of order h but not a restricted basis of any order. Evidently some kind of divisibility condition must be imposed upon a basis to force it to be a restricted basis.

In this paper we discuss the case $h = 2$, for which the above counter-example is invalid. We shall prove the following theorems:

THEOREM I. *A basis of order 2 is a restricted basis of order at most 4.*

THEOREM II. *An asymptotic basis of order 2 is a restricted basis of order at most 3 if the value of its counting function is, for a suitable positive constant C, larger than $Cx/\log\log x$ for all sufficiently large x.*

(The value of the counting function of a set of integers is the number of integers in the set $\leqq x$; here x is a non-negative real number.)

It is possible that every basis, or even every asymptotic basis, of order 2 is a restricted basis of order at most 3, but we have been unable to establish

---

* Received June 21, 1956; revised January 3, 1957.

this. As another simple example shows, this result, if true, is best possible: The set of integers whose representations in the ternary scale have only the digits 0 and 1 is a basis of order 2 but not a restricted basis of order 2.

Our proof of Theorem I is elementary. It involves certain lemmas which bear somewhat upon a famous conjecture of Erdös and Turán [2]. Apart from the use that is made of Roth's celebrated theorem on progression-free sequences [3], our proof of Theorem II is also elementary.

2. The main lemmas. Let A be a basis of order 2 with elements a_i, $i=1,2,3,\cdots$. By a' we shall mean the smallest element in A which is larger than a. If x is an arbitrary integer, we shall mean by $\rho(x)$ the number of representations of x as the sum of two elements of A, where the representations $x=a_i+a_j$ and $x=a_j+a_i$ will be regarded as distinct when $i\neq j$.

Theorem I is an easy consequence of the following lemmas:

LEMMA 1. *If A is a basis of order 2, there exists an even integer x such that $\rho(x)\geqq 4$.*

LEMMA 2. *If A is a basis of order 2, then either there exists an odd integer y such that $\rho(y)\geqq 4$ or A is one of the two sets*

$$(0,1,3,\cdots,2n+1,\cdots),\quad (0,1,2,4,\cdots,2n,\cdots).$$

In 1941, Erdös and Turán conjectured that $\limsup \rho(n)=\infty$ for asymptotic bases. Either Lemma 1 or Lemma 2 implies that, for bases, l. u. b. $\rho(n)\geqq 4$. Actually, this can be shown directly, and more simply, using the method employed in proving Lemmas 1 and 2.

3. Proof of Lemma 1. We shall show, in order to prove Lemma 1, that the assumption that every even number has no more than 3 representations as a sum of two integers of a basis, A, of order 2, leads to a contradiction. Our method involves a cumbersome consideration of various cases. Clearly $0\in A$, $1\in A$ and either 2 or 3 or both are in A.

Case 1. $2\in A$, $3\in A$. Here $3'\neq 4$, for otherwise $\rho(4)>3$. If $3'=5$, then $5'=9$, for $5'<9\rightarrow\rho(8)>3$ while $5'>9\rightarrow\rho(9)=0$. Similarly $9'=13$. But now $\rho(14)=4$; hence $3'\neq 5$. If $3'=6$, then $6'\geqq 9$, for $6'<9\rightarrow\rho(8)>3$. If $6'=9$, one sees, arguing in the same way, that the next elements in A must be 13, 17, and 21; but then $\rho(30) > 3$. Therefore $6' = 10$, for otherwise $\rho(10) = 0$. As before, the next elements in A must be 17, 21, 25 and 29; but then $\rho(46) > 3$. Thus $3' \neq 6$. Consequently $3' = 7$, for otherwise $\rho(7) = 0$. But now $7' = 11$ and $11' = 15$ and we have $\rho(18) > 3$. We have shown that A cannot contain both 2 and 3.

Case 2. $2 \in A$, $3 \notin A$. If $2' = 4$, then $4' = 7$ and $7' \geqq 9$. If $7' = 9$, then 10, 12, 14, 15 and 16 are not in A, for then $\rho(16) > 3$ or $\rho(10) > 3$. Thus $9' = 11$, since otherwise $\rho(12) = 0$. $11' \neq 13$, for then $\rho(20) > 3$. Hence $11' = 17$, since otherwise $\rho(17) = 0$. But now $\rho(18) > 3$. Hence $7' \neq 9$. Thus $7' = 10$, otherwise $\rho(10) = 0$. 11 and 12 are not in A, for then $\rho(12) > 3$. $13 \notin A$, for then $\rho(14) > 3$. But now $\rho(13) = 0$. Hence $2' \neq 4$.

It follows that $2' = 5$, for otherwise $\rho(5) = 0$. Now $5' \neq 6$, for then $\rho(6) > 3$. If $5' = 7$, then $7' \geqq 9$. If $7' = 9$, then 10, 11, and 12 are not in A, for then $\rho(12) > 3$. Also, $13 \notin A$, for then $\rho(14) > 3$. But now $\rho(13) = 0$. Hence $7' \neq 9$. If $7' = 10$ or $7' = 11$, then $\rho(12) > 3$. Hence $7' > 11$. But now $\rho(11) = 0$. Thus $5' \neq 7$. Consequently $5' = 8$, for otherwise $\rho(8) = 0. 8' \geqq 11$, for otherwise $\rho(10) > 3$. But if $8' > 11$, then $\rho(11) = 0$; hence $8' = 11$. $11' \geqq 13$, for otherwise $\rho(12) > 3$. If $11' = 13$, then one can see that 14, 15, 16 and 17 are not in A, for the presence of any one of these would make $\rho(14) > 3$ or $\rho(16) > 3$ or $\rho(18) > 3$. But now $\rho(17) = 0$. Hence $11' = 14$, for otherwise $\rho(14) = 0$. But now $\rho(16) > 3$. Thus the case $2 \in A$, $3 \notin A$ cannot occur.

Case 3. $2 \notin A$, $3 \in A$. $3' \neq 4$; otherwise $\rho(4) > 3$. Thus $3' = 5$, as otherwise $\rho(5) = 0$. $5' \neq 6$, for then $\rho(6) > 3$. Hence $5' = 7$, as otherwise $\rho(7) = 0$. But now $\rho(8) > 3$. This completes the proof of Lemma 1.

4. Proof of Lemma 2. Let A be a basis of order 2 and suppose that every odd number has exactly 2 representations as the sum of 2 elements of A. As before, $0 \in A$ and $1 \in A$.

Case 1. $2 \in A$. We show that there are no larger odd numbers in A. Suppose the contrary. Let $2m + 1$, $m \geqq 1$, be the smallest odd number, apart from 1, in A. Then A must contain all even numbers between 2 and $2m - 2$ inclusive, for otherwise the odd numbers between 3 and $2m - 1$ would have no representations. It is also clear that $2m \notin A$. Since every odd number $\leqq 4m - 1$ now has two representations, it follows that

$(2m+1)' > 4m-1$. But then $\rho(4m-2)=0$, unless $m=1$ or $m=2$. The case $m=1$ is excluded immediately, since here $\rho(3)>2$. In the latter case, $2'=5$, and $5'=8$. Clearly $9 \notin A$; also $11 \notin A$, as otherwise $\rho(13)>2$. Hence $8'=10$, for otherwise $\rho(11)=0$. 12 and 13 are not in A, for then $\rho(13)>2$. $14 \notin A$, for then $\rho(15)>2$. But now $\rho(14)=0$.

Thus the only odd element of A in this case is 1. It follows that all even numbers must be in A; that is, A is the set $(0,1,2,\cdots,2n,\cdots)$.

Case 2. $2 \notin A$. We show that all remaining elements of A are odd. Suppose the contrary. Let $2m$, $m \geqq 2$, be the smallest even element of A, apart from 0. Then A must contain all odd numbers $\leqq 2m-1$. It follows, as before, that $(2m)'=4m$ or $(2m)'=4m+1$. If $(2m)'=4m$, then $(4m)'>4m+2$, as otherwise $\rho(4m+1)>2$ or $\rho(4m+3)>2$. But now $\rho(4m+2)=0$.

Hence $(2m)'=4m+1$. By the same arguments as before we infer that A contains all odd numbers in the closed interval $[4m+1, 6m-1]$ and no even numbers in this interval. All odd numbers less than $8m-1$ are now represented as sums of elements of A; it follows that there are no integers in A in the closed interval, $[6m, 8m-1]$. $8m \in A$; otherwise $\rho(8m)=0$. All odd numbers up to $10m-1$ now having 2 representations, there are no elements of A between $8m$ and $10m-1$. Either $(8m)'=10m$ or $(8m)'=10m+1$; in the contrary case $\rho(10m+1)=0$.

If $(8m)'=10m$, then all odd numbers $\leqq 14m-1$ have two representations; $(10m)' \geqq 14m$. But now $\rho(12m+2)=0$. Hence $(8m)'=10m+1$. But now $\rho(12m+1)>2$.

Thus all elements of A, apart from 0, are odd; A is the set $(0,1,3,5,\cdots)$.

5. Proof of Theorem I. Let A be a basis of order 2 and let z be an arbitrary odd positive integer larger than $3x$, where x is the even integer mentioned in Lemma 1. Then $z-x$ is odd and we may write $z-x=a_1+a_2$, since A is a basis of order 2, with $a_1 \neq a_2$. Since $\rho(x) \geqq 4$, we have $x=a_3+a_4=a_5+a_6$, where no two of the integers a_3, a_4, a_5, a_6 are the same. Since $z-x$ is larger than $2x$, at most one of the integers a_1, a_2 is less than or equal to x. Hence at most one of them can be equal to one of the integers a_3, a_4, a_5, a_6. Suppose, for example, that $a_1=a_3$. Then we have $z=a_1+a_2+a_5+a_6$ with all summands distinct.

In a similar fashion, using Lemma 2, we can treat the case in which

z is an arbitrary even integer larger than $3y$. Theorem I is obviously true for the exceptional bases mentioned in Lemma 2.

It has been pointed out by the referee that Theorem I is immediate if one knows that $\rho(n) < n^{1/3}/6^{2/3}$. For in this case we have for large n,

$$A^2(\tfrac{1}{2}n) < \sum_{j=0}^{n} \rho(n) < n^{4/3}/6^{2/3}, \text{ whence } A(\tfrac{1}{2}n) < n^{2/3}/6^{1/3}.$$

If $\lambda(n)$ denotes the number of representations of n as the sum of four elements of A with at least one repetition, then

$$\lambda(n) \leqq 6 \sum_{A} \rho(n-2j) \leqq 6A(\tfrac{1}{2}n)\rho(n) < n.$$

But, since A is a basis of order 2, the total number of representations of n as the sum of 4 elements of A is at least n.

6. Progressive-free sets. Let $B = (b_1, b_2, \cdots, b_r)$ be a set of distinct positive integers. B is said to be a progression-free set if the equation $2b_k = b_i + b_j$ has no solution with $i \neq j$. Let x be a positive real number and let $B(x)$ denote the maximum number of integers in any progression-free set of whose elements are less than x. Roth's theorem states that $B(x) = O(x/\log\log x)$.

Let S be any set of non-negative integers and let T be the set of integers which can be represented as the sum of 2 elements in S in just one way, namely as $2s_i$, $s_i \in S$. Then T is progression free, for $2(2s_i) = 2s_j + 2s_k$ implies $2s_i = s_j + s_k$, so that $i = j = k$.

If $B = (b_1, b_2, \cdots, b_r)$ is progression-free the set $C = (c_1, c_2, \cdots, c_r)$, where $c_i = \lambda b_i + \mu$, $\lambda \neq 0$, $i = 1, 2, \cdots, r$, also contains no arithmetic progressions.

7. Chains. We turn now to the proof of Theorem II. Let A be an asymptotic basis of order 2. Suppose that every integer larger than t can be represented as the sum of 2 elements of A. Let x be an integer greater than t which cannot be represented as the sum of 3 distinct elements of A. If $a_p \in A$, $a_p \leqq x$, then, since A is an asymptotic basis of order 2, either $x - a_p \leqq t$ or $x - a_p = 2a_q$ with $a_q \in A$ or $x - a_p = a_p + a_r$ with $a_r \in A$, whence $x - a_r = 2a_p$. By an x-chain we mean a collection of elements $a_1, a_2, \cdots, a_k$ in A such that

$$(1) \qquad x - a_1 = 2a_2, x - a_2 = 2a_3, \cdots, x - a_{k-1} = 2a_k,$$

where the equations $x - a_e = 2a_1$ and $x - a_k = 2a_m$ with $a_e \in A$, $a_m \in A$ have no solutions. It is clear that, with at most t exceptions, every element in A which is $\leqq x$ belongs to one and only one x-chain.

Using the standard method for solving a linear difference equation, one can easily show that

$$(2)\qquad a_n = \tfrac{2}{3}(x-3a_1)(-\tfrac{1}{2})^n + \tfrac{1}{3}x; \qquad n = 1, 2, \cdots, k.$$

It follows from (2) that, except for the case $a_1 = x/3$ the elements of a chain are distinct. The number of distinct elements in a chain will be called its length and will be denoted by k.

Putting $n = k$ in (2) we see that since a_k is an integer, $x - 3a_1$ must be divisible by 2^{k-1}. A chain will be said to be associated with m if $x - 3a_1$ is exactly divisible by 2^m. Clearly, if $a_1 \neq x/3$, $k \leqq m+1$; also $m \leqq u = [\log x/\log 2] + 1$. In case $a_1 = x/3$, we shall put $k = 1$, $m = 0$.

The integer $x - a_1$ has only the representation $x - a_1 = 2a_2$ as the sum of two elements of A, for $x - a_1 = a_1 + a_e$ would imply $x - a_e = 2a_1$ and a_1 would not be the initial element of its x-chain. From our remarks in (6) it follows that the initial elements of all x-chains form a progression-free set.

The initial elements of the x-chains associated with m also form a progression-free set. So do the integers of the form $(x-3a_1)/2^m$ where a_1 runs over all the initial elements of chains associated with m. These integers must lie between $-x/2^{m-1}$ and $x/2^m$, that is, in an interval of length $3x/2^m$. If we let $\alpha(m)$ denote the number of x-chains associated with m then

$$(3)\qquad \alpha(m) \leqq B(3x/2^m).$$

Similarly, the total number of x-chains is $\leqq B(x)$.

8. Proof of Theorem II. We have

$$A(x) \leqq t + \sum k \leqq t + \sum (m+1) \leqq t + \sum_{m=0}^{u} m\alpha(m) + \sum 1,$$

where the unindexed summations are taken over all x-chains. Putting $v = [\log x/2\log 2]$ and employing (3) we have

$$A(x) \leqq t + \sum_{m=0}^{v} mB(3x/2^m) + \sum_{m=v+1}^{u} mB(3x/2^m) + B(x).$$

Using Roth's theorem, we have

$$\begin{aligned} A(x) &\leqq t + \sum_{m=0}^{v} 3c_1 mx/2^m \log\log(3x/2^m) + \sum_{m=v+1}^{u} mB(3x^{\frac{1}{2}}) + c_1 x/\log\log x \\ &\leqq t + \sum_{m=0}^{v} 3c_1 mx/2^m \log\log(3x^{\frac{1}{2}}) + 3x^{\frac{1}{2}} \sum_{m=v+1}^{u} m + c_1 x/\log\log x \\ &\leqq t + c_2 x/\log\log x \sum_{m=0}^{\infty} m/2^m + c_3 x^{\frac{1}{2}} \log^2 x + c_1 x/\log\log x \end{aligned}$$

$\leqq t + c_4 x/\log\log x$, where c_1, c_2, c_3 and c_4 are absolute constants. Since x was an integer which could not be represented as the sum of 3 distinct elements of A, it is clear that our last inequalty implies Theorem II.

MICHIGAN STATE UNIVERSITY.

REFERENCES.

[1] G. Pall, "On sums of squares," *American Mathematical Monthly*, vol. 40 (1933), pp. 10-18.

[2] P. Erdös and P. Turán, "On a problem of Sidon in additive number theory and some related problems," *Journal of the London Mathematical Society*, vol. 16 (1941), pp. 212-215.

[3] K. F. Roth, "On certain sets of integers," *Journal of the London Mathematical Society*, vol. 28 (1953), pp. 104-109.

ORDINARY DIFFERENTIAL EQUATIONS AND LAPLACE TRANSFORMS.*

By AUREL WINTNER.

PART I.

On the case of integrability by Laplace transforms which corresponds to the Fuchsian case of a singular point of a linear differential equation.

1. Let $f(z)$ be regular on the half-plane $\operatorname{Re} z > 0$, and let $f(z)$ be representable as a Laplace-Stieltjes transform

$$f(z) = \int_0^\infty e^{-zt}\, d\alpha(t) \tag{1}$$

$(0 \leqq t < \infty)$ which is *absolutely* convergent for $\operatorname{Re} z > 0$. Then the function $f(z)$ will be called *of class* (A) (more specifically, of class (A_0), where the subscript refers to the abscissa of the boundary line), and its $\alpha = \alpha(t)$ will be denoted by $\alpha_f = \alpha_f(t)$. It is understood that $\alpha(t)$ is uniquely determined by $f(z)$ only after the normalization of an additive constant and of the values of $\alpha(t)$ at its discontinuity points (for instance, if $\alpha(0) = 0$ and $\alpha(t+0) = \alpha(t)$, where $0 \leqq t < \infty$); and that $\alpha_f(t)$ is of bounded variation on every finite interval $0 \leqq t \leqq T$ but need not stay bounded as $t \to \infty$, since (1) need not converge at $z = 0$. It is clear that

$$f(z) \to \alpha_f(+0) - \alpha_f(0) \quad \text{as } \operatorname{Re} z \to \infty, \tag{1 bis}$$

and that $f(z)$ is bounded for $\operatorname{Re} z > \epsilon$ if $\epsilon > 0$.

Consider the solutions $w = w(z)$ of the differential equation

$$w'' + f(z) w = 0, \tag{2}$$

and let the trivial solution $w(z) \equiv 0$ (which is of class (A), with $\alpha_w(t) \equiv 0$) be excluded. Then, if $f(z)$ is of class (A), there need not exist any solution $w(z)$ of class (A) (or, for that matter, of class (A_r), no matter how large $r > 0$ be chosen, where $g(z)$ is called of class (A_r) if $g(z - r)$ is of class $(A_0) = (A)$). In order to see this, choose $\alpha_f(t) = \frac{1}{2}t^2$. Then (1) is of

---

* Received September 27, 1956.

class (A) and reduces (2) to $w'' + w/z^2 = 0$. But this differential equation is satisfied (for $\operatorname{Re} z > 0$) by $w(z) = z^a$, where a is either root of $a(a-1)+1 = 0$; so that, since $\operatorname{Re} a = \frac{1}{2} > 0$ holds for both roots a, no solution $w(z)$ stays bounded as $Rz \to \infty$, and so no solution is of class (A) (or, for that matter, of class (A_r) for some $r > 0$).

It will turn out that this trivial counterexample is close to the border of that subclass of the functions $f(z)$ of class (A) for which the possibility of a counterexample becomes replaced by an existence statement. For, on one hand, such a subclass will prove to be characterized by the condition

$$\int_0^1 t^{-2} \, | \, da_f(t) \, | < \infty \tag{3}$$

(which is a local condition for $t \to 0$, since it is equivalent to

$$a_f(+0) = a_f(0) \tag{3 bis}$$

and $\int_\delta^\eta t^{-2} \, | \, da_f(t) \, | \to 0$ together, where $0 < \min(\delta, \eta) \to 0$). And, on the other hand, (3) is "just barely" (logarithmically) violated by the $a_f(t) = \frac{1}{2}t^2$ of the preceding counterexample $f(z)$.

2. It was shown in [7] that if $f(z)$, besides being of class (A), is such as to belong to an $a_f(t)$ which, for a sufficiently small $\epsilon > 0$, satisfies the condition

$$a_f(t) = \text{const. if } 0 \leqq t < \epsilon, \tag{4}$$

then (2) has a solution $w(z)$ of class (A), and that this $w(z)$ is substantially unique (by this is meant that this $w(z)$ can be replaced only by $cw(z)$, where c is just one of the two integration constants of (2)). But it was also shown in [7] that the restriction (4) of the coefficient function of (2) will compel the (A)-solution $w(z)$ of (2) to be such as to satisy $a_w(t) = \text{Const.}$ for $0 \leqq t < \epsilon$ (where ϵ is the same constant as in (4)). Correspondingly, the assumption (4) played the drastic part of completely eliminating "small divisors" (not "diophantine" small divisors, of the type occurring in celestial mechanics, but still "small divisors", entering in the discussion of the solution of the differential equation in the same way, and creating the same "resonance" trouble, as in celestial mechanics).

It was shown in [8] that if (2) is replaced by a system, say (S), of n homogeneous, linear differential equations of first order, with a coefficient matrix $F(z)$ all n^2 elements of which are of class (A), then the drastic assumption corresponding to the case $f=F$ of (4) can be improved to an integral condition on the behavior of $a_F(t)$ near $t=0$, a condition characterizing the allowable amount of "small divisors." But this problem on (S) is quite different from that of (2), since that integral condition on $a_F(t)$ refers to the systems (S) for which all (vector) solutions are of class (A), whereas (2), when written in the form (S) (with $n=2$), can never have this property (correspondingly, $f(z)\equiv 1$ will be one of the $n^2=4$ of the elements of the resulting (S), and $f(z)\equiv 1$ belongs to $a_f(t)=\operatorname{sgn} t$ in (1); so that (3 bis) is violated). On the other hand, if an appropriate transcription of the method of [8] is attempted from (S) to (2), then the convergence of the successive approximations is made to depend on estimates which, though obtainable, become too involved.

In what follows, all these difficulties will be avoided by having recourse to function-theoretical arguments. Instead of applying, as in [7] and [8], successive approximations in the a-space, the successive approximations will be carried out *before* the application of the Laplace transformation. The necessary estimates then become of the classical type. But what is needed is their translation to the a-space. This can, however, be handled by an appeal to the theory of normal families, since the "translation" process is then taken care of by the "continuity theorem" of the transform (1) (where $f=f, w, w_k$; $k=1,2,\cdots$). Thus the proof becomes a counterpart (for Laplace transforms) of the corresponding treatment of the spectral resolution (which is an isue concerning Stieltjes transforms, instead of Laplace transforms); cf. [4], pp. 104-105 and pp. 171-173.

3. What will thus result is the following theorem:

If both coefficient functions $g(z)$, $f(z)$ *of*

$$w''+g(z)w'+f(z)w=0, \tag{5}$$

where $\operatorname{Re} z>0$, *are of class* (A), *and if their* (*Laplace-Stieltjes*) *Unterfunktionen* $a_f(t)$, $a_g(t)$, *where* $0\leqq t<\infty$, *behave, near* $t=0$, *so as to satisfy the respective "small divisor" restrictions*

$$\int_0^1 t^{-1}\,|\,da_g(t)\,|<\infty, \qquad \int_0^1 t^{-2}\,|\,da_f(t)\,|<\infty, \tag{6}$$

then, on the half-plane $\operatorname{Re} z>0$, *the general solution of* (5) *is of the form*

$$w(z)=c_1zu(z)+c_2v(z), \tag{7}$$

where the function $u(z)$ *(which is not a solution) and the function* $v(z)$ *(which is a solution* $w(z)$ *belonging to* $c_1 = 0$*) are of class* (A).

The structure of the two conditions (6), when compared with Fuchs' classical theorem on differential equations (5) for which $z = 0$ is a "regular" singular point (cf., e. g., [1], p. 120), explains the choice of the title of this Part I. In this regard, cf. also Bôcher's extension [2] of Fuchs' sufficient condition to the real field, particularly the case dealing with the case corresponding to a multiple elementary divisor, and the remark made in the footnote on p. 854 of [6].

Corresponding to the Fuchsian parallelism, it is clear how the assumption and the assertion of the theorems (and it will be obvious from the nature of the proof below how the proof of the theorem) can be extended from $n = 2$ to any n, if n is the order of the homogeneous, linear differential equation $D(w) = 0$. If $n = 1$, then the theorem is trivial; cf. [8], p. 174. This trivial case also shows that the "Fuchsian" integral conditions of the general theorem cannot (in general) be improved (in this regard, cf. also the Appendix of [5]). The theorem resulting for an arbitrary n is a "small divisor" refinement of the corresponding result of [3], where (4) is assumed for all n coefficient functions $f(z)$ of $D(w) = w^{(n)} + \cdots + f_0(z)w$.

In order to halve the length of the formulae, the proof of the italicized theorem will be given for the case $g(z) \equiv 0$ only. Then (5) and (6) reduce to (2) and (3) respectively. It will be clear from the proof that the modifications needed in it when $g(z) \not\equiv 0$ are of a trivial nature. Actually, the unessential assumption $g(z) \equiv 0$ will shorten the proof only insofar as it will make possible the use of some of the passages in [5] and [6].

4. Instead of the analytic differential equation (2), consider first the differential equation

$$w'' + f(x)w = 0 \tag{8}$$

($' = d/dx$) in which $f(x)$ is a (possibly complex-valued) continuous function of the real variable x, defined for large positive x in such a way that $xf(x)$ is absolutely integrable or, what is the same thing, that

$$F(x) \to 0 \text{ as } x \to \infty, \tag{9}$$

where

$$F(x) = \int_x^\infty s\,|f(s)|\,ds. \tag{10}$$

Under these assumptions on $f(x)$, the following facts are contained in Bôcher's paper [2] implicitly (cf. the remark on [2] made in Section 3 above), and in [5] explicitly (and, incidentally, under an assumption requiring of f somewhat less than the absolute integrability of xf):

(i) The differential equation (8) has a solution $w(x)$ satisfying the "initial condition"

$$w(x) \to 1 \text{ as } x \to \infty, \tag{11}$$

and this solution of (8) is unique.

(ii) On the half-line on which $f(x)$ is given, all the integrals occurring in the recursion formula

$$w_n(x) = 1 + \int_x^\infty (x - s) f(s) w_{n-1}(s)\, ds, \tag{12}$$

where $n = 1, 2, \cdots$ and

$$w_1(x) \equiv 0, \tag{13}$$

are absolutely convergent, and the differences of consecutive functions in the sequence

$$w_1(x), \cdots, w_n(x), \cdots \tag{14}$$

are subject, at every point x of that half-line, to the inequality

$$| w_n(x) - w_{n-1}(x) | \leqq (G(x) + F(x))^n, \tag{15}$$

where

$$G(x) = \int_x^\infty | f(s) |\, ds \tag{16}$$

(hence $G(x) \leqq F(x)$ if $x \geqq 1$, by (10)).

(iii) As a consequence of (ii), *the solution* $w(z)$, *assigned by* (11) *in* (i), *can be obtained by the process of successive approximations on some half-line* $x_0 < x < \infty$ (if x_0 is large enough, so large that, in (15),

$$G(x) + F(x) < 1 \text{ if } x_0 < x < \infty; \tag{17}$$

and (9) and the parenthetical remark made after (16) assure the existence of an x_0 satisfying (17)).

The refinement (iii) of (i), along with (ii) (where $x > x_0$ is *not* assumed) will be essential in what follows. The finite x-interval which is debarred by the proviso $x > x_0$ of (iii) will prove to be such that its inclusion becomes possible if an appropriate use is made of (ii).

5. Now consider (2) under the assumption that, on the (open) half-plane $x > 0$, where x is the real part of $z = x + iy$, the coefficient function $f(z)$ is regular and representable as an absolutely convergent integral (1) (that is, that $f(z)$ is of class (A)), and identify (2) with (8), by keeping y fixed in $z = x + iy$, where

$$0 < x < \infty \tag{18}$$

and $-\infty < y < \infty$. Then what correspond to (12), (13) and (14) are

$$w_n(z) = 1 + \int_z^\infty (z - s)\{\int_0^\infty e^{-st} d\alpha_f(t)\} w_{n-1}(s)\, ds, \tag{19}$$

with

$$w_1(z) \equiv 0, \tag{20}$$

and

$$w_1(z), \cdots, w_n(z), \cdots. \tag{21}$$

Similarly, (15) becomes

$$|w_n(z) - w_{n-1}(z)| \leqq (G(x) + F(x))^n, \tag{22}$$

where, corresponding to (10) and (16),

$$F(x) = \underset{-\infty < y < \infty}{\text{l. u. b.}} \left| \int_z^\infty \left| s \int_0^\infty e^{-st}\, d\alpha_f(t) \right| ds \right| \tag{23}$$

and

$$G(x) = \underset{-\infty < y < \infty}{\text{l. u. b.}} \left| \int_z^\infty - \int_0^\infty e^{-st} d\alpha_f(t) \right| ds \,|. \tag{24}$$

It follows from (i) that (2) will have a unique solution $w(z)$ satisfying the limit relation

$$w(z) \rightarrow 1 \text{ as } x \rightarrow \infty \tag{25}$$

(which is meant to be uniform for $-\infty < y < \infty$), if the condition corresponding to the convergence of the integral (10), where $x > 0$, is satisfied by f. This will certainly be the case if the expression (23) is finite at every point of the half-line $x > 0$. But it is clear that if (23) is replaced by

$$(26)\qquad F(x)=\int_x^\infty)s\int_0^\infty e^{-st}\,|\,d\alpha_f(t)\,|)ds,$$

then (23) is finite if (26) is (at a given $x>0$) and that, under the latter assumption,

$$(27)\qquad G(x)=\int_x^\infty (\int_0^\infty e^{-st}\,|\,d\alpha_f(t)\,|)ds$$

is finite; finally, that (22) remains true if (as always in the sequel) the functions $F(x)$, $G(x)$ are defined by (26) and (27), rather than by (23), (24).

Accordingly, (i) and (ii) become applicable on (18) if (26) is convergent on (18). But (26), where x, s, t are positive, can be rearranged into

$$(28)\qquad F(x)=\int_0^\infty e^{-xt}(1+tx)t^{-2}\,|\,d\alpha_f(t)\,|$$

(since $t^2\int_x^\infty se^{-st}ds=(1+tx)e^{-st}$, and since Fubini's theorem on product measures is applicable whether the integrals are finite or not) and, correspondingly, (27) can be written in the form

$$(29)\qquad G(x)=\int_0^\infty e^{-xt}t^{-1}\,|\,d\alpha_f(t)\,|.$$

On the other hand, since (1) is supposed to converge absolutely if $x>0$, it is clear that (28) will be finite for every $x>0$ if and only if (3) is satisfied (and that (29) is then certainly finite for every $x>0$). But (3) is an assumption of the italicized theorem, to be proved.

Consequently, (i) and (ii) can be applied in the following proof of the theorem. In view of (i), it is already assured that (2) has a unique solution $w(z)$ satisfying (25). This solution exists, as a regular function, on the half-plane $x>0$, since, by the local existence theorem of (analytic) linear differential equations, every solution of (2) is regular on every z-domain on which the coefficient function $f(z)$ is regular. What remains to be seen is that the particular solution $w(z)$, defined by (25), is a Laplace-Stieltjes transform, and that the latter is absolutely convergent on the entire half-plane $x>0$ (and not, as one might expect from (iii), only on some half-plane $x>x_0$, where x_0 is sufficiently large).

6. To this end, (ii) will have to be used in the form obtained in Section 5, a form which states that (27), (26) and (19) satisfy (15) for $n = 1, 2, \cdots$ and at every point z of the half-plane $x > 0$.

It is clear from (ii) that each of the functions (21), defined by (19) and (20), is a regular function on the half-plane $x > 0$. This information will be completed by the following pair of facts:

(I) The sequence (21) is uniformly bounded on every fixed half-plane $x > \epsilon$, where $\epsilon > 0$.

(II) Each of the functions (21) is of class (A), that is, a Laplace-Stieltjes integral, say

$$w_n(z) = \int_0^\infty e^{-zt} d\beta_n(t), \tag{30}$$

which is absolutely convergent on the half-plane $x > 0$.

If (I) and (II) are granted, then it is possible to proceed as follows: According to (iii), there exists a half-plane $x > x_0$ on which the sequence (21) tends to the solution $w(z)$ determined by (25). But it follows from (I) that, in view of the theory of normal families, the "sufficiently large" x_0 can be improved to any $\epsilon > 0$. If this is combined with (II), it follows that the functions (21), besides being absolutely convergent integrals (30) on the half-plane $x > 0$, form a sequence which is uniformly bounded and (uniformly) convergent on every half-plane $x > \epsilon$, where $\epsilon > 0$ is arbitrary. But the assumptions placed on $f(z)$ in (2) are such as to remain satisfied if (2) is replaced by

$$w'' + f^*(z) w = 0 \text{ or } w'' - f^*(z) w = 0,$$

where

$$f^*(z) = \int_0^\infty e^{-zt} \, | d\alpha_f(t) | \text{ for } x > 0;$$

cf. (1). Hence it is clear from (19) and (20) that not only the functions (30) but also the functions

$$w_n^*(z) = \int_0^\infty e^{-zt} \, | d\beta_n(t) |$$

form a sequence which is uniformly bounded and (uniformly) convergent on every half-plane $x > \epsilon$, where $\epsilon > 0$. It follows therefore from the "continuity theorem" of Laplace-Stieltjes transforms that, if $v(z)$ is the limit function of the sequence (30) (that is, if $v(z)$ denotes the solution $w(z)$ of (2) defined by (25)), then $v(z)$ is a Laplace-Stieltjes transform, say

$$(31) \qquad v(z) = \int_0^\infty e^{-zt} d\beta(t),$$

which is absolutely convergent on the half-plane $x > 0$. In fact, if the constant $\beta_n(0)$, which (30) leaves undetermined for every n, is suitably chosen, then $w_n(z) \to v(z)$ as $n \to \infty$ (for $x > 0$) is equivalent to $\beta_n(t) \to \beta(t)$ as $n \to \infty$ in (30) and (31) (if the discontinuity points of $\beta(t)$ are disregarded).

Accordingly, the existence of the (unique) solution $w(z)$ which in (7) belongs to $(c_1, c_2) = (0, 1)$ follows if (I) and (II) are granted. On the other hand, if the existence of the solution $v(z)$ is granted, then the existence of the solution $zu(z)$, a solution $w(z)$ which belongs to $(c_1, c_2) = (1, 0)$ in (7), follows by the argument applied in [7], pp. 448-450. Consequently, the proof of the theorem will be complete if (I) and (II) are proved.

7. Clearly, each of the (complex) functions (19), where $z = x + iy$ and $x > 0$, is majorized by the corresponding (real, non-negative), function

$$(32) \qquad W_n(x) = 1 + \int_x^\infty (s - x) \{ \int_0^\infty e^{-st} \, | d\alpha_f(t) | \} W_{n-1}(s) \, ds,$$

where $0 < x < \infty$ and, corresponding to (20),

$$(33) \qquad W_1(z) \equiv 0.$$

Hence (I) will be proved if it is shown that the functions (32) are uniformly bounded on every closed half-line contained in the open half-line (18).

For similar reasons, (II) will follow if it is shown that each of the functions (32) is a Laplace-Stieltjes integral which is absolutely convergent on (18). Hence, somewhat more than (II) will be proved if it is shown that

(34) $W_n(x)$ is completely monotone on (18).

In fact, (34) and the Hausdorff-Bernstein theorem imply that if $\gamma_n(t)$ belongs to $W_n(x)$ in the same way as $\alpha(t)$ belongs to $f(z)$ in (1), then not only does there exist on (18) a Laplace-Stieltjes representation of $W_n(x)$ in terms of $\gamma_n(t)$ but, in addition, $d\gamma_n(t) \geqq 0$. But it also follows from the Hausdorff-Bernstein theorem that (34) is equivalent to the following assertion:

$$(35_n) \qquad (-D)^m W_n(x) \geqq 0, \text{ where } m = 0, 1, \cdots \text{ and } 0 < x < \infty$$

$(D = d/dx)$. Hence (II) is true if $(35_1), (35_2), \cdots$ are true.

Since (35_1) is clear from (33), it follows that (II) will be proved if it is shown that (35_{n-1}) implies (35_n). This induction will be carried out now. The proof of (I) will be deferred to Section 8.

First, it is clear from Section 6 that each of the integrals (32) is convergent on (18). Next, (32) and a differentiation of (32) show that the cases $m = 0$ and $m = 1$ of (35_{n-1}) imply the cases $m = 0$ and $m = 1$ of (35_n). Hence, when proving that (35_{n-1}) implies (35_n), it is sufficient to consider the cases $m = 2, 3, \cdots$ of (35_n). But two differentiations of (32) show that

$$D^2 W_n(x) = W_{n-1}(x) \int_0^\infty e^{-xt} \,|\, d\alpha_f(t) \,|.$$

It follows therefore from (35_{n-1}), and from the fact that the product of two functions which are completely monotone on (18) is completely monotone on (18), that $D^2 W_n(x)$ is completely monotone on (18). Since this means that the cases $m = 2, 3, \cdots$ of (35_n) are true, the induction is complete.

8. In view of the end of Section 6 and of the beginning of Section 7, all that remains to be proved is that the functions (32) are uniformly bounded on every half-line $\epsilon < x < \infty$, where $\epsilon > 0$ is arbitrary.

Let (32) be written in the form

$$(36) \qquad W_n(x) = 1 + \int_x^\infty (s - x) f^*(s) W_{n-1}(s)\, ds,$$

where

$$(37) \qquad f^*(x) = \int_0^\infty e^{-xt} \,|\, d\alpha_f(t) \,|.$$

If Fubini's theorem is applied in the same way as in Section 6, then it is clear from (37) that (3) and the absolute convergence of (3) and (18) together are equivalent to the (absolute) convergence of

$$(38) \qquad \int_0^\infty t f^*(x + t)\, dt \qquad (f^* \geqq 0).$$

for every $x > 0$. Hence, the assertion is that (36), where $W_1(x) \equiv 0$, and the convergence of (38) on (18) imply the existence of a constant $C = C(\epsilon)$ satisfying

$$W_n(x) < C(\epsilon) \text{ for } \epsilon < x < \infty, \tag{39}$$

whenever $\epsilon > 0$. (All that is clear is that there exists a bound, depending on n, for which

$$W_n(x) < C_n(\epsilon) \text{ if } \epsilon < x < \infty; \tag{39 bis}$$

simply because each of the integrals (36) is convergent on (18).)

Since (36), where $W_1(x) \equiv 0$, implies that $W_2(x) \equiv 1$, it is clear that if

$$U_n(x) = W_n(x) - W_{n-1}(x), \tag{40}$$

then $U_1(x) \equiv 1$ and $U_n(x) = \int\limits_x^\infty (s - x) f^*(s) U_{n-1}(s) \, ds$, that is,

$$U_n(x) = \int\limits_0^\infty s f^*(x + s) U_{n-1}(x + s) \, ds. \tag{41}$$

The iteration of (41) shows that $U_{n+1}(x)$ is the n-fold integral

$$U_{n+1}(x) = \int\limits_0^\infty \cdots \int\limits_0^\infty \prod_{k=1}^n s_k f^*(x + s_1 + s_2 + \cdots + s_k) \, ds_k. \tag{42}$$

But since both (non-negative) integrals (37), (38) are convergent for every $x > 0$, it can readily be concluded from (42) that the functions $U_1(x)$, $U_2(x), \cdots$ are uniformly bounded on every fixed half-line $\epsilon < x < \infty$, where $\epsilon > 0$. In view of (40), where $W_1(x) \equiv 0$ and $W_2(x) \equiv 1$, this is equivalent to (39).

PART II.

Ordinary non-linear differential equations and Laplace transforms.

Introduction. The following considerations deal with three questions, (α), (β) and (γ), on families $x = x(t, c)$ of solutions of differential equations $dx/dt = f(t, x)$, where c is an integration constant, confined to a "sufficiently small" c-domain, and (A) if t is real, its range is either (a) a fixed interval which is not compact, say $0 \leqq t < \infty$, or (b) a half-line $T \leqq t < \infty$ with a $T = T_c$ which cannot be chosen independent of c, whereas (B) in the analytic case, the t-range is either (a) a fixed half-strip ($0 \leqq \operatorname{Re} t < \infty$, $|\operatorname{Im} z| <$ const.) or (b) a half-strip ($T \leqq \operatorname{Re} t < \infty$, $|\operatorname{Im} t| < \epsilon$) with $T = T_c$ and $\epsilon = \epsilon_c$.

In each of the four cases (Aa), (Ab), (Ba), (Bb), the three questions to be considered are (α) the existence of $x(t, c)$ on the infinite t-range, (β) the uniform continuity of $x(t, c)$ in t and c together (which, since the t-range is infinite, is equivalent to the question of stability in the sense of Dirichlet), finally (γ) the representation of $x(t) = x(t, c)$ as a Laplace-Stieltjes integral (the subcase (γA) of (γ) subsumes itself to the subcase (γB)). If (α_1), (α_2), (α_3) denote (α), (β), (γ) respectively, then the issue is the specification of conditions which, when satisfied by f, are sufficient for (α_i), where i is fixed. The resulting conditions will of course be stricter for (α_{i+1}) than for (α_i).

It will be sufficient to deal with the case in which x or f is a scalar. In fact, it will be clear from the nature of the proofs that the vector case (that is, the case of a system $dx_j/dt = f_j(t, x_1, \cdots, x_n)$, where $j = 1, \cdots, n$) can be reduced to the scalar case by a device of superordination, a device which reduces to the prinicple of majorization in the analytic case. Actually, the proofs are such as to make it clear that a direct treatment of the vectorial case differs from that of the scalar case in hardly more than in the intepretation of the symbols.

1. Suppose first that the f of

$$dx/dt = f(t, x) \tag{1}$$

is real-valued and continuous on the half $t \geqq 0$ of a real (t, x)-plane. Suppose further that

$$\int^{\infty} |f(t, 0)|\, dt < \infty, \tag{2}$$

and that there exists on the half-line $t \geqq 0$ a non-negative, continuous (but not necessarily bounded) function $\lambda(t)$ which satisfies the condition

$$\int^{\infty} \lambda(t)\, dt < \infty \tag{3}$$

and which is a "global Lipschitz factor" of f; that is, for which

$$|f(t, x') - f(t, x'')| \leqq \lambda(t)\, |x' - x''| \tag{4}$$

holds for any pair (t, x'), (t, x'') of points (t, x) contained in the half-plane

$$(5) \qquad 0 \leqq t < \infty, \qquad -\infty < x < \infty.$$

Under these assumptions, (1) is "unrestricted," that is, every solution $x = x(t)$ of (1) exists for

$$(6) \qquad 0 \leqq t < \infty.$$

What is more, every solution $x(t)$ of (1) tends, as $t \rightarrow \infty$, to a finite limit, $x(\infty)$. Conversely, if there is given any point c of the line

$$(7) \qquad -\infty < c < \infty,$$

then there exists an initial condition x_0 corresponding to which the solution $x(t)$ determined $x(0) = x_0$ has the limit $x(\infty) = c$. These (and certain more general) facts were proved in [10]; for extensions, cf. the Appendix of this paper.

As pointed out to me by Professor Siegel (cf. [10], pp. 131-132), the correspondence between the $x(0)$-line and the $x(\infty)$-line is continuous and one-to-one in the general solution of (1), that is, by virtue of

$$(8) \qquad x = x(t, x_0); \qquad x(0, x_0) = x_0, \qquad \lim_{t \rightarrow \infty} x(t, x_0) = x(\infty; x_0).$$

2. In what follows, it will be very essential that, under the assumptions (2)-(5), it is possible to choose a t^* in such a way that, on the portion

$$(9) \qquad t^* \leqq t < \infty$$

of the half-line (6), the solutions $x(t) = x(t; c)$ *of* (1) can be obtained by the following process of sucessive approximations:

$$(10) \qquad x_{n+1}(t) = c - \int_t^\infty f(s, x_n(s))\, ds,$$

where c is the arbitrary "initial constant" $x(\infty)$, the iteration process (10) starts with

$$(11) \qquad x_0(t) \equiv c \qquad\qquad (c = x(\infty)),$$

and the convergence (in fact, even the absolute convergence) of each of the integrals (10) on the half-line (9) is part of the statement. In other words, the half-line (9) can be chosen in such a way that the sequence

$$(12) \qquad x_0(t), x_1(t), \cdots, x_n(t), \cdots$$

will be defined by (11) and (10) and will converge on (9) (as a matter of fact, uniformly on (9)) to that solution $x(t)$ of (1) which belongs to $x(\infty)=c$. In fact, this was the "non-local" part of the proof in [10] (but not in [12], where nothing like a Lipschitz condition is assumed).

By adapting an argument which is well-known in the classical "local" problem (Bendixson-Lindelöf), it can be shown that (12) converges not only on a certain (constant) portion (9) of (6) but on the whole of (6), that is, for $0 \leqq t \leqq t^*$ as well. But this will not be needed in what follows.

3. In order to apply the (vectorial variants of the) facts collected in Section 1 to the problem of vortices and nodes (Poincaré), a simple device had to be applied in [14], pp. 821-823. In what follows, the adaptation of that device will be needed, in order to deal with the case in which the half-plane (5) of f is replaced by a strip

$$(13) \qquad 0 \leqq t < \infty, \qquad -b < x < b,$$

where $b > 0$ is given arbitrarily (it can be "small").

Suppose that $f(t,x)$ is real-valued and continuous on (13) and satisfies (2) and (4), with (3), on (13). Then, corresponding to every positive b_0 which is less than b, there exist a sufficiently small $b^* = b^*(b_0) > 0$, a sufficiently small $c^* = c^*(b_0)$ and a sufficiently large $t^* = t^*(b) \geqq 0$ which have the following properties: Every solution $x(t)$ of (1) which belongs to any initial condition $x(t^*) = x^*$ satisfying

$$(14) \qquad |x^*| < b^* \qquad (x^* = x(t) \text{ at } t = t^*)$$

exists on (9), satisfies

$$(15) \qquad |x(t)| < b_0$$

on (9), and tends, as $t \to \infty$, to a limit c satisfying

$$(16) \qquad |c| < c^* \qquad (c = x(\infty)).$$

Conversely, there belongs to every c satisfying (16) a unique solution $x(t)$ of (1) which exists on (9), satisfies the inequality (15) on (9) and the conditions $c = x(\infty)$ and (14), where $x^* = x(t^*)$ (note that $b^* > 0$ can be chosen arbitrarily small; in particular, so as to be less than b_0). Finally, for every c satisfying (16), not only (15) but also

$$(17) \qquad |x_n(t)| < b_0 \qquad (n = 0, 1, \cdots)$$

holds on (9), where the functions (12) are defined, on (9), by (11) and

(10) and converge, on (9), to that solution $x(t)$ of (1) which is determined by the "initial condition" $x(\infty)=c$.

First, since $0<b_0<b$, and since $f(t,x)$ is given on (13) as a continuous function satisfying (2) and (4), with (3), it is clear that if (13_0) denotes the strip which results if b is replaced by b_0 in (13), then it is possible to choose on the half-plane (5) a continuous $f(t,x)$ which is identical with the given $f(t,x)$ on the portion (13_0) of (13) and which satisfies (2) and (4), with (3), on (5). Hence, all the assertions, concerning the existence of the positive numbers b^*, c^*, t^* which have the above-stated properties, follow from Sections 1-2 and from the very nature of the process of the sucessive approximations (cf. [10]).

4. It is also clear from the nature of the successive approximations that nothing is changed if the real differential equation (1) is replaced by the complex differential equation

$$dw/dz=f(z,w), \tag{18}$$

where, corresponding to the continuity of $f(t,x)$ on the strip (13), the function $f(z,w)$ is supposed to be regular on

$$\operatorname{Re} z>0, \qquad |w|<b, \tag{19}$$

the product space of a circle $|w|<b$ and of the half-plane $x>0$, where $z=x+iy$, $-\infty<y<\infty$. Then there exists on (19) an absolutely convergent expansion

$$f(z,w)=\sum_{m=0}^{\infty} f_m(z)w^m, \tag{20}$$

where every

$$f_m(z) \text{ is regular for } x>0 \qquad (x=\operatorname{Re} z). \tag{21}$$

What corresponds to (2) is the condition

$$\int^{\infty} \underset{-\infty<y<\infty}{\text{l. u. b.}} |f_0(x+iy)|\,dx<\infty. \tag{22}$$

Similarly, what corresponds to (4) and (3) on (13) is certainly satisfied if

$$\int^{\infty} \underset{-\infty<y<\infty}{\text{l. u. b.}}\, h(x+iy)dy<\infty, \text{ where } h(z)=\underset{|w|<b}{\text{l. u. b.}} |f(z,w)/w)| \tag{23}$$

(provided that the integrand of (23) is continuous (and $\neq\infty$) at every x). Incidentally, less than this proviso would suffice in (23); cf. [13]).

These are all the assumptions which correspond to those of Section 3. Hence, under these assumptions, there will belong to every circle $|z|<b_0$, where $0<b_0<b$, a half-plane $\operatorname{Re} z>d^*$, a circle $|w_0|<b^*$ $(\leqq b_0)$, where $w_0=w(z)$ at $z=z_0$ and $\operatorname{Re} z_0>d^*$, and a circle $|c|<c^*$, where $c=w(\infty)$, in such a way that the assertions of Section 3 hold (in their complex version). It is understood that $w(\infty)=c$ now means that $w(x+iy)\rightarrow c$ holds uniformly for $-\infty<y<\infty$ as $x\rightarrow\infty$.

5. As an application, choose on the half-line

$$0\leqq s<\infty \tag{24}$$

a sequence of functions $a_0(s), a_1(s),\cdots$ satisfying $[a_m]<\infty$, where $m=0, 1,\cdots$ and

$$[a]=\int_0^\infty |da(s)|. \tag{25}$$

Then (21) is certainly satisfied if

$$f_m(z)=\int_0^\infty e^{-zs}da_m(s), \tag{26}$$

and (20) is certainly regular on (19) if

$$\sum_{m=0}^{\infty}[a_m]b^m<\infty, \text{ where } [a_m]=\int_0^\infty |a_m(s)|. \tag{27}$$

Actually, these assumptions are much stricter than necessary; suffice it to say that, for every fixed m, the integral (26) can have a finite abscissa of boundedness and uniform convergence without having a finite abscissa of absolute convergence.

In view of the case $m=0$ of (26), and since

$$\int_1^\infty s^{-1}|da(s)|\leqq\int_1^\infty |da(s)|\leqq[a]<\infty,$$

condition (22) is certainly satisfied if

$$\int_0^1 s^{-1}|da_0(s)|<\infty. \tag{28 bis}$$

On the other hand, since it is clear from (20) and (26) that the function $h(z)$ occurring in (23) is

$$h(z) = \underset{|w|<b}{\text{l. u. b.}} \left| \sum_{m=1}^{\infty} m w^{m-1} \int_0^{\infty} e^{-zs} da_m(s) \right| \leqq \sum_{m=1}^{\infty} m b^{m-1} \int_0^{\infty} e^{-xs} \, | da_m(s) |,$$

condition (23) is certainly satisfied if

$$\sum_{m=1}^{\infty} m b^m \int_0^1 s^{-1} \, | da_m(s) | < \infty .$$

Hence, if the notation is changed so as to replace the given $b > 0$ by a somewhat greater $b > 0$, it is clear that (23) is satisfied if

$$\sum_{m=1}^{\infty} b^m \int_0^R s^{-1} \, | da_m(s) | < \infty$$

holds for $R = \infty$ or, what in view of (27) is the same thing, for $R = 1$. Finally, since $m > 0$ in the last sum, it follows that not only condition (23) but also condition (22) (which belongs to $m = 0$ and was taken care of by (28 bis) above) will be satisfied if, in addition to (27),

$$(28) \qquad \sum_{m=0}^{\infty} \{a_m\} b^m < \infty, \text{ where } \{a_m\} = \int_0^1 s^{-1} \, | da_m(s) | .$$

[Note that $a_m(+0) = a_m(0)$, where $m = 0, 1, \cdots$, is a necessary condition for (28).]

Accordingly, the situation is as follows: If the coefficient functions of (20) are of the form (26) and satisfy (27) and (28) for some $b > 0$ (that is, if $[a_m]^{1/m}$ and $\{a_m\}^{1/m}$, where $m = 0, 1, \cdots$ and $1/0 = 1$, are less than a constant), then the results of Section 4 are applicable to (18).

This implies, among other things, that there will exist a sufficiently large $d^* > 0$ and a sufficiently small $b^* > 0$ in such a way that, whenever z_0 and w_0 are numbers satisfying

$$(29) \qquad \operatorname{Re} z_0 > d^* \text{ and } | w_0 | < b^*$$

respectively, the initial condition

$$(30) \qquad w(z_0) = w_0$$

will determine a solution

$$w = w(z) = w(z; z_0, w_0) \tag{31}$$

of

$$dw/dz = \sum_{m=0}^{\infty} w^m \int_0^{\infty} e^{-zs} d\alpha_m(s) \tag{32}$$

which exists (as a regular function) on the half-plane

$$\operatorname{Re} z > \operatorname{Re} z_0, \tag{33}$$

and each of these solutions (31) will tend to a finite limit $c = c(z_0, w_0)$:

$$w(z) \to c \text{ as } \operatorname{Re} z \to \infty. \tag{34}$$

In addition, these solutions $w(z)$ can be obtained (if b^* and $1/d^*$ are small enough) by the following process of successive approximations:

$$\lim_{n\to\infty} w_n(z) = w(z) \text{ on } (33), \tag{35}$$

where the sequence

$$w_0(z), w_1(z), \cdots, w_n(z), \cdots \tag{36}$$

is defined, corresponding to (11) and (12), by

$$w_{n+1}(z) = c - \int_z^{\infty} \sum_{m=0}^{\infty} f_m(\zeta)(w_n(\zeta))^m d\zeta \qquad \text{[cf. (26)]} \tag{37}$$

and

$$w_0(z) \equiv c \qquad (c = w(\infty)) \tag{38}$$

together, and the integrals (37) are convergent on (33) and represent regular functions satisfying

$$|w_n(z)| < b \text{ on } (33); \tag{39}$$

cf. (17).

6. On this basis, the following theorem will now be proved:

Let $f_0(z), f_1(z), \cdots$, *where* $\operatorname{Re} z > 0$, *be a sequence of functions* (26) *satisfying* (27) *and* (28) *for some* $b > 0$, *and let* $f(z, w)$ *be defined by* (20) *on the domain* (19). *Suppose further that* $f_0(z) \equiv 0$. *Then there exist two positive numbers,* d^* *and* b^* $(\leqq b)$, *having the following properties: If* z_0 *and* w_0 *are complex numbers within the circle* $|z_0| < b^*$ *and the half-plane*

$\operatorname{Re} z_0 > d^*$ *respectively, then the solution* $w = w(z) = w(z; z_0, w_0)$ *of the (local) initial-value problem*

$$dw/dz = f(z, w), \qquad w(z_0) = w_0$$

exists on the half-plane $\operatorname{Re} z > d^*$ *and is representable as a Laplace-Stieltjes integral*

$$w(z) = \int_0^\infty e^{-zs} d\beta(s) \tag{40}$$

which is absolutely convergent for $\operatorname{Re} z > d^*$; *in addition,*

$$|w(z)| < b \text{ for } \operatorname{Re} z > d^*. \tag{40 bis}$$

Needless to say, the function $\beta(s)$ occurring in (40) depends on the initial constant $w(z_0) = w_0$ (and is of bounded variation on every finite interval of the half-line $0 \leqq s < \infty$).

Theorems of this type are known under substantially stricter assumptions. In fact, the known results deal either with linear differential equations (cf. [8]) or, in the non-linear case typified by (32), assume (cf. [9]) that

$$a_m(s) \equiv 0 \text{ for } 0 \leqq s \leqq 1, \text{ where } m = 0, 1, \cdots \tag{41}$$

(if the unit of length is suitably chosen on the half-line (24) and if the functions $a_m(s)$, in which (26) leaves undetermined an additive constant, are normalized by $a_m(1) = 0$). But (41) is a very drastic way of satisfying (28), whereas (if (27) is assumed) the allowable behavior of the functions $a_m(s)$ *near* $s = 0$ is the main issue. In fact, what is involved is a problem in "small divisors" (cf. Part I, Section 2, above).

On the other hand, (27) and (28) are the true conditions. In order to see this, it is sufficient to consider the particular case in which (32) becomes homogeneous and linear, that is,

$$dw/dz = f(z)w, \text{ with } f(z) = \int_0^\infty e^{-zs} da(s), \tag{42}$$

where $a_m \equiv 0$ if $m \neq 1$ and $a_1 = a$. Then (27) and (28) reduce to

$$\int_0^\infty |da(s)| < \infty \text{ and } \int_0^1 s^{-1} |da(s)| ds < \infty. \tag{43}$$

But if $da(s) \geqq 0$ (that is, if $da = |da|$), then a quadrature shows that (42) cannot possess any solution $w(z) \not\equiv 0$, representable for sufficiently large

$\operatorname{Re} z$ as an (absolutely) convergent integral (40), unless both conditions (43) are satisfied.

The proof for the sufficiency of (27) and (28) seems to call for elaborate estimates of the total variations of the successive approximations to the (unknown) function $\beta(s)$ which occurs in (40). It turns out however that this elaborate work (which, in my first attempts to prove the sufficiency of (27) and (28), appeared to be too involved to be completed by explicit induction) can be avoided entirely. This will be made possible by an appeal to the "continuity theorem" of the transform (40) (cf. the end of Section 2 in Part I).

7. It will be clear from the proof of the italicized theorem that, for reasons of majorization, it is sufficient to prove the theorem for the case in which the functions $a_m(s)$ occurring in (26), (27), (28) are real-valued and non-decreasing (so that $da_m(s) = |da_m(s)|$ for $m = 0, 1, \cdots$ and $0 \leqq s < \infty$) and, in addition, the circle $|w_0| < b^*$ and the half-plane $\operatorname{Re} z_0 > d^*$ of the initial conditions are replaced by the interval $0 \leqq w_0 < b^*$ and the half-line $d^* < z_0 < \infty$ respectively. For the same reason, it will be sufficient to consider the differential equation (32) and the existence of its solution (40) only on the half-line $d^* < x < \infty$, where $x = \operatorname{Re} z$ (correspondingly, z_0 will be denoted by x_0). Then it is clear from the way in which the results of Section 5 were obtained that $c \geqq 0$ in (34).

The c of (34) is the same as the c of the recursion formulae (37)-(38). Since $da_m(s) = |da_m(s)|$ in (26), these recursion formulae now become

$$(44) \qquad w_{n+1}(x) = c - \int_x^\infty \sum_{m=0}^\infty \Big(\int_0^\infty e^{-ts} \, |da_m(s)| \Big) (w_n(t))^m dt,$$

where $0 < d^* < x_0 \leqq x < \infty$ and

$$(45) \qquad w_0(x) = c \geqq 0 \qquad (c = w(\infty)).$$

If d^* and b^* are so chosen as in Section 5 (in connection with (29)), and if c is small enough (with reefrence to d^* and b^*), then, according to Sections 4-5, all integrals (44) (which in view of (45) have non-negative integrands) exist ($< \infty$) on the half-line

$$(46) \qquad x_0 < x < \infty$$

and satisfy the limit relation

$$(47) \qquad \lim_{n \to \infty} w_n(x) = w(x) \text{ on } (46), \text{ where } w(\infty) = c,$$

where $w(x)$ is a solution of $dw/dx = f(x, w)$. Hence, in view of the concluding sentence of Section 6, the italicized theorem will be proved if it is shown that each of the functions $w_n(x)$ is representable in the form

$$(48) \qquad w_n(x) = \int_0^\infty e^{-xs} d\beta_n(s) \text{ on } (46), \text{ where } d\beta_n(s) \geqq 0.$$

But this can be shown by an adaptation of the corresponding step in Part I.

In fact, the assertion of (48) is equivalent to the statement that each of the functions $w_n(x)$ is completely monotone on (46), that is, that, if $D = d\ /dx$,

$$(49_n) \qquad (-D)^k w_n(x) \geqq 0 \text{ on } (46), \text{ where } k = 0, 1, \cdots$$

(Hausdorff-Bernstein). Since the truth of (49_0) is clear from (45), it is sufficient to prove that (49_{n+1}) is implied by (49_n). But (45) and the case $n = 0$ of (44) show that the case $k = 0$ of the inequalities (49_n) is true for every n. On the other hand, differentiation of (44) shows that

$$(50) \qquad -Dw_{n+1}(x) = \sum_{m=0}^{\infty} \Big(\int_0^\infty e^{-xs} \,|\, da_m(s) \,|\Big) (w_n(x))^m.$$

Since $-Df(x)$, $g_1(x) + g_2(x)$ and $\lim f_m(x)$, where $m \to \infty$, are completely monotone on (46) if $f(x)$, $g_j(x)$ and $f_m(x)$ are (provided that $\lim f_m(x)$ exists), it follows by successive differeniations of (50) that (49_n) is true for every n and every m if every (49_n) is true for $m = 0$ (cf. the corresponding induction in Section 7 of Part I).

8. Accordingly, all that remains to be verified is the case $k = 0$ of (49_n) for every n, that is,

$$(51_n) \qquad w_n(x) \geqq 0 \text{ on } (46).$$

Since (51_0) is clear from (45), it is sufficient to prove that (51_{n+1}) is implied by (51_n). This induction will prove (49_n) for every n if $c > 0$ in (45). The limiting case $c = 0$ will have to be discussed separately.

Suppose first that $c > 0$. Then, since the integral occurring in (44) (for a fixed n) is convergent for $d^* < x < \infty$ (where $d^* < x_0$), it is clear from (44) that $w_{n+1}(x) > 0$ is true for every x which is large enough with reference to c and $n + 1$. But (50) holds on the *fixed* half-line (46), since $x_0 > d^*$. Since the truth of (51_n) is assumed (for a fixed n), it follows that $Dw_{n+1}(x) \leqq 0$ on (46). Consequently, (51_{n+1}) follows from the fact that

$w_{n+1}(x) \geqq 0$ is true for *large* x (it also follows that the sign of equality cannot take place in (51_n) for any n).

In the remaining case, $c = 0$. But the assumption $f_0(z) \equiv 0$ of the italicized theorem (Section 6), an assumption which reduces (20) to

$$f(z, w) = \sum_{m=1}^{\infty} f_m(z) w^m, \tag{52}$$

was not used thus far. If it *is* used, then it is clear that (18) admits the solution $w(z) \equiv 0$. Since the latter belongs to the case $c = 0$ of (34), and can be represented in the form (40), with $d\beta(s) \equiv 0$, the proof is complete.

9. Since the assumption that (20) reduces to (52) was used nowhere but in the last paragraph of Section 8, the following theorem was also proved above:

Let $f_0(z), f_1(z), \cdots$, *where* $\operatorname{Re} z > 0$, *be a sequence of functions* (26) *satisfying* (27) *and* (28) *for some* $b > 0$. *Then, if* $r = r(b) > 0$ *is sufficiently small and if* c *denotes any complex number satisfying* $0 < |c| < r$, *there exists an abscissa* $d = d(c) < \infty$ *having the following properties: The differential equation* (18) *has a solution* $w(z) = w(z; c)$ *which exists on the half-plane* $\operatorname{Re} z > d$, *satisfies the "initial condition"* (34), *and is representable on the half-plane* $\operatorname{Re} z > d$ *as an absolutely convergent Laplace-Stieltjes integral* (40), *where* $\beta(s) = \beta_c(s)$ (*and* $w(z)$ *satisfies the inequality* $|w(z)| < b$ *if* $\operatorname{Re} z > d$).

Since $c = 0$ is excluded, it is clear from (34) and (40) that $\beta(s) = \beta_c(s)$ has a jump $(= c = \beta(+0) - \beta(0) \neq 0)$ at $s \neq 0$.

APPENDIX.

On a non-local theory of the initial value problem of ordinary differential equations.

1. Let H_0 denote the open half-line $0 < t < \infty$, H the closure of H_0, R the n-dimensional x-space $(-\infty < x_i < \infty; i = 1, \cdots, n)$, with $x = (x_1, \cdots, x_n)$ and $|x| = (x_1^2 + \cdots + x_n^2)^{\frac{1}{2}}$, and $f(t, x)$ a vector function, with n real components, which is defined and continuous (but not necessarily uniformly continuous or bounded) on $H \times R$. According to Peano,

$$dx/dt = f(t, x) \tag{1}$$

defines a (local) flow. The state of R under this flow at the date t will be denoted by R_t; so that R_0 is the space R of all initial conditions x_0 which can be assigned for a (not necessarily unique) solution $x(t)$ of (1) as $x(0) = x_0$. Eventually, under appropriate restrictions of the given function $f(t, x)$ (cf. (C) below), even the state R_∞ of R will be considered.

In [10]-[13] I investigated various non-local issues concerning the solutions $x = x(t; x_0)$ of (1) (when f is subject to appropriate restrictions); that is, issues pertaining to the existence and behavior of $x(t; x_0)$ on the whole of H (and for any point x_0 of R), rather than just on some "sufficiently small" t-interval. The main questions can be listed as follows:

Type (A). Every solution $x(t; x_0)$ of (1) should be "unrestricted," that is, such as to be "continuable" for $0 \leqq t < \infty$ (the standard example in which such is *not* the case is Riccati's scalar differential equation $x' = x^2$, possessing the solution $x(t) = -(t - t_0)^{-1}$ which exists for $0 \leqq t < t_0$ if $0 < t_0 < \infty$ but cannot be extended into any solution for $0 \leqq t < t^0$ if $t^0 > t_0$).

Type (A*). Let (1) be of type (A) and such as to possess the property that $\limsup |x(t; x_0)| < \infty$, where $t \to \infty$, holds for every solution ("stability" for every fixed x_0). A refinement of this type is

Type (B). Let (1) be of type (A) and such as to possess the property that, corresponding to every solution $x(t; x_0)$, there exists a point $c = c(x_0)$ of R satisfying $x(t; x_0) \to \infty$ as $t \to \infty$ (this will be expressed by saying that $x(\infty; x_0)$ exists on R_0).

Type (B*). Let (1) be of type (A) and such that there exists, as $t \to \infty$, a finite $\lim |x(t)|$ for the *length* of every solution under $x(t)$ of (1) (this condition, concerning *amplitudinal* limits, requires more than (A*) but less than (B)).

Type (C). Let (1) be of type (B) and such as to possess the property that every point of R is the $x(\infty; x_0)$ of at least one point x_0 of R_0 (so that one can speak of R_∞).

Type (D). Let (1) be of type (C) and such as to possess the property that the correspondence between R_0 and R_∞, that is, the mapping $x_0 \to x(\infty; x_0)$, is continuous and one-to-one.

Type (D bis). Let (1) be of type (A) and such as to possess the property that $x(t; x_0) \to 0$, as $t \to \infty$, holds for every solution. This type is of type (B) but represents just the opposite of type (C). A variant of this "confluent" type (in which the point, 0, of "confluence" could of course be replaced by any point of R) is

Type (D*). Let (1) be of type (A) and such as to possess the property that $|x(t;x_0)| \to 0$, as $t \to \infty$, holds for every solution (this type is just the opposite of type (A*)).

The issue is the specification of conditions which, when satisfied by the given function $f(t,x)$, assure that (1) belongs to one of these types. Such criteria were given *loc. cit.* In what follows, the results available to the methods applied there will be systematized and further developed.

2. The starting point for any non-local statement (that is, of a statement on H) must be the following lemma (cf. [11], and [18], p. 177):

LEMMA. *If there is given for* (1), *where* $f(t,x)$ *is continuous on* $H \times R$, *a solution* $x(t)$ *on an interval* $0 \leqq t < t_0$, *where* $t_0 < \infty$, *then either there exists some interval* $0 \leqq t < t^0$, *where* $t^0 > t_0$, *on which* (1) *possesses some solution which is identical with the given solution for* $0 \leqq t < t_0$ *or else* $|x(t)| \to \infty$ *holds as* $t \to t_0 - 0$ [in which case the "non-continuability" of the given solution, that is, the non-existence of any $t^0 > t_0$, is clear from the fact that a function $x(t)$ cannot satisfy (1) at $t = t_0$ if it is not differentiable at t_0; hence certainly not if it fails to be bounded near t_0].

The alternative implies that $\liminf |x(t)| < \infty$, where $t \to t_0 - 0$, assures the existence of $\lim |x(t)|$ and, what is more, the existence of $\lim x(t)$; and that $\limsup |x(t)| = \infty$ cannot hold unless $\lim |x(t)| = \infty$. The latter point is the crucial step in the proof of the Lemma, which in [11] I abstracted from Painlevé's (and Weierstrass') considerations on the singularities of the problem of three bodies (Weierstrass's investigations are of an earlier date, but were published, posthumously, much later, than those of Painlevé; cf. [16] and [17]).

By a generalization of the argument applied in the Appendix of [11], a generaliaztion suggested by a local criterion of Kamke [15], pp. 139-141, the following comparison theorem can be derived from the Lemma:

(i) *Let* $f(t,x)$ *be continuous on* $H \times R$ *and, if* H_0 *and* J *denote the open half-line* $0 < t < \infty$ *and the closed half-line* $0 \leqq r < \infty$ *respectively, let there exist on* $H_0 \times J$ *a continuous function* $g(t,r)$ *satisfying*

$$(2) \qquad |f(t,x)| \leqq g(t,|x|) \text{ on } H_0 \times R \qquad (g \geqq 0)$$

and having the following property: If any solution $r=r(t)$ *of*

$$(3)\qquad dr/dt=g(t,r)$$

is given on any t-interval I contained in H_0 *(with* $(t,r(t))$ *in* $I\times J$*), then there exists on* H_0 *a function* $r(t)$ *(with* $(t,r(t))$ *in* $H_0\times J$*) which is a solution of* (3) *on* H_0 *and reduces to the given* $r(t)$ *on I. Then* (1) *is of type* (A).

The proof of this (A)-criterion will be such as to supply the following (A*)-criterion also:

(i*) *Let f and g satisfy the assumptions of* (i). *Suppose further that* $\limsup r(t)<\infty$, *where* $t\to\infty$, *holds for every solution* $r(t)$ $(\geqq 0)$ *of* (3). *Then* (1) *is of type* (A*).

The assertion of the Lemma is that any solution $x(t)$ of (i), given for small $t-t_0\geqq 0$, where t_0 $(\geqq 0)$ is fixed, can be extended to a solution of (1) on H. It will be sufficient to prove the existence of such an extension for $t_0\leqq t<\infty$. Suppose that there does not exist such an extension. Then, by the Lemma, there is a finite $t^0>t_0$ having the property that $x(t)$ exists, but is not bounded, on the interval $t_0\leqq t<t^0$. Consider a solution $r=r(t)$ of (3) belonging to the initial condition $r(t_0)=r_0$, where $r_0=|x(t_0)|$. According to the assumption made in (i) on (3), the solution $r(t)$ will exist on H_0 and will, therefore, be bounded on $t_0\leqq t<t^0$. But (1), (2), (3) and $|x(t_0)|=r(t_0)$ imply that $|x(t)|\leqq r(t)$ for $t_0\leqq t<t^0$; hence $x(t)$ remains bounded as $t\to t^0-0$. This contradiction proves (i).

It is also seen that $|x(t)|\leqq r(t)$ for $t_0\leqq t<\infty$. Since this inequality holds whether the additional assumption of (i*) is satisfied or not, (i*) follows.

A particular useful corollary of (i), a corollary in which the assumptions which (i) posits for $g(t,r)$ become replaced by "explicit" assumptions, is the following:

(i_0) *Let* $f(t,x)$ *be continuous on* $H\times R$ *and let there exist, on the respective open half-lines* $(0<t<\infty)$, $(0<r<\infty)$, *two positive, continuous functions* $\lambda=\lambda(t)$, $\phi=\phi(r)$ *satisfying*

$$(4)\qquad |f(t,x)|\leqq\lambda(t)\phi(r)\ \text{ on } H_0\times R$$

and

$$(5)\qquad \int_1^\infty dr\,/\phi(r)=\infty.$$

Then (1) *is of type* (A).

This can be reduced to the criterion proved in the Appendix of [11] if the dt of (1) is replaced by $\lambda(t)dt$ and, when the old t in $f(t,x)$, where $f=(f_1,\cdots,f_n)$ and $x=(x_1,\cdots,x_n)$, is denoted by x_0, the n-ary system (1) is replaced by the $(n+1)$-ary system $dx^*/dt=f^*(x^*)$, where $x^*=(x_0,x)$ and $f^*=(1,f)$. Actually, (i_0) is a particular case of (i). In fact, if $g(t,r)=\lambda(t,r)$, then (2) and (3) become (4) and

$$dr/dt=\lambda(t)\phi(r) \tag{6}$$

respectively. But if (6) is written in the form $dr/\phi(r)=\lambda(t)dt$ (when $r>0$, hence $\phi(r)>0$), and if it is observed that $\lambda(t)$ stays between positive bounds on compact subintervals of H_0, then it is seen from (5) that the condition required of (3) in (i) is satisfied by (6).

3. The (A)-criterion (i_0) has the following (B)-counterpart:

(ii) *If the assumptions of* (i_0) *are satisfied and if, in addition,*

$$\int_1^\infty \lambda(t)dt<\infty, \tag{7}$$

then (1) *is of type* (B).

In fact, (ii) can be concluded from (i_0) in about the same way as (i_0) was concluded from (i); cf. [12].

A (C)-counterpart of (i) is as follows:

(iii) *If the assumptions of* (ii) *are satisfied and if, in addition,*

$$|f(t,x')-f(t,x'')|\leqq\lambda(t)\phi(|x'-x''|) \text{ on* } H_0\times R'\times R'' \tag{8}$$

and

$$\int_{+0}^\infty |f(t,0)|\,dt<\infty, \tag{9}$$

then (1) *is of type* (C).

This was proved in [13]. Actually, (iii) can be concluded from (ii) in about the same way as (ii) is concluded from (i_0).

(iii^0) *If the assumptions of* (iii) *are satisfied and if, in addition,* (7) *is supplemented by*

$$\int_\epsilon^1 \lambda(t)dt<\infty, \tag{10}$$

---

* By R' and R'' are meant the x-space R when $x=x'$ and $x=x''$ respectively.

and (5) *by*

$$(11)\qquad \int_{\epsilon}^{1} dr\ /\phi(r) = \infty,$$

finally (8) *by*

$$(12)\qquad |f(0,x') - f(0,x'')| \leqq \phi(|x' - x''|) \text{ on } R' \times R'',$$

then there belongs to every point (t_0, x_0) *of* $H \times R$ *only one solution* $x(t)$ *of* (1) *satisfying* $x(t_0) = x_0$.

In fact, what (iii^0) adds to (iii) is a purely local statement, and the latter is nothing but Osgood's well-known criterion for local uniqueness; cf. [15], p. 100 and p. 142. On the other hand, something very different from this local assertion is contained in the following (D)-counterpart of the (C)-criterion (iii):

(iv) *If the assumptions of* (iii^0) *are satisfied, then* (1) *is of type* (D).

It is clear from the definition of the (D)-type that the truth of (iv) presupposes the truth of (iii^0).

The case $\phi(r) = r$ of (iv) was concluded by Siegel (cf. [10], pp. 131-132) from the proof of the case $\phi(r) = r$ of (iii) (cf. [10], pp. 125-131) by a simple topological argument. But a glance at that argument shows that nothing is changed if $\phi(r) = r$ is replaced by any $\phi(r)$ satisfying (5) and (11).

4. The (B*)-character of (1) (that is, the existence of finite *amplitudinal* limits) can be assured by an assumption on f which, in contrast to the preceding "bilateral" assumptions, is just "unilateral":

(ii*) *Let* $f(t,x)$ *be continuous on* $H \times R$ *and suppose that*

$$(13)\qquad x \cdot f(t,x) \leqq 0 \text{ on } H_0 \times R,$$

(*where* $x \cdot f = x_1 f_1 + \cdots + x_m f_m$) *or, more generally, that there exists on* H_0 *a non-negative* $\lambda(t)$ *satisfying*

$$(14)\qquad \int_{\epsilon}^{\infty} \lambda(t)\,dt < \infty \text{ if } \epsilon > 0$$

and

$$(15)\qquad (x \cdot f(t,x))^+ \leqq \lambda(t) \min(1, |x|^2) \text{ on } H_0 \times R$$

(*where* $(x \cdot f)^+ = \max(0, a)$ *for* $a = x \cdot f$). *Then* (1) *is of type* (B*).

Remark. The choice of the term $\phi(|x|^2) = |x|^2$ in the factor min of $\lambda(t)$ in (15) corresponds to the particular case $\phi(r) = r$ in the preceding criteria. Correspondingly, it will be clear from the proof of (ii*) how to extend (ii*) to other choices of $\phi(|x|^2)$. The choice $\phi(|x|^2) = |x|^2$, made in (ii*) for the sake of simplicity, is important in the theory of *linear* systems $(1)_*$; cf. [13], pp. 558-559, or [19].

In order to prove (ii*), put $\frac{1}{2}|x|^2 = s = s(t)$ along any solution $x = x(t)$ of (1) which is given on an interval $0 \leqq t < t_0$. Consider first the particular case (13) of (15) (cf. [13], p. 557). Then scalar multiplication of (1) by x shows that $ds(t) \leqq 0$ if $0 \leqq t < t_0$. Hence $s(t_0 - 0) = \infty$ is impossible if $t_0 < \infty$, and so the Lemma assures that t_0 can be assumed to be ∞; so that (1) is of type (A). But then it is clear from $ds(t) \leqq 0$ and $s(t) \geqq 0$ that there must exist a finite $s(\infty) \geqq 0$; that is, that there must exist for $x(t)$ an amplitudinal limit, which is the (B*)-assertion of (ii*).

Next, replace (13) by (15) but suppose, in addition to (15), that

$$x \cdot f(t \cdot x) \geqq 0 \text{ on } H_0 \times R. \tag{16}$$

Then it follows from (1) that, if $0 \leqq t < t_0$ (where, for the present, $t_0 = \infty$ *or* $t_0 < \infty$), then

$$0 \leqq ds(t)/dt \leqq \lambda(t) \min(1, s(t)). \tag{17}$$

Since $ds/s = d \log s$, it is clear from (17) and (14) that there cannot exist a finite t_0 satisfying $s(t_0 - 0) = \infty$, and so, for the same reason as before, (1) must be of type (A). But then, by letting $t \to \infty$ in (17), and using $ds/s = d \log s$ and (14) again, one is led to the existence of a finite $s(\infty) > 0$, provided that $s(t) = \frac{1}{2}|x(t)|^2$ does not vanish for large t.

If $s(t) > 0$ only on a sequence of (open) t-intervals $I_1, I_2, \cdots$ which cluster at $t = \infty$, but $s(t) = 0$ on the (closed) set K complementary to $L = I_1 + I_2 + \cdots$, then the existence of a finite $\lim s(t)$ follows if t tends to ∞ so as to be confined to $I_1^* + I_2^* + \cdots = L^* = L^*(\epsilon_1, \epsilon_2 \cdots)$, where $I_n^* = I_n^*(\epsilon_n)$ denotes, for any positive $\epsilon_n < 1$, an interval contained in I_n and having a length $|I_n^*| < (1 - \epsilon_n)|I_n|$. But the value of $\lim s(t)$, with t on L^*, is independent of the choice of L^*, since L^* is in L for every choice of $\epsilon_1, \epsilon_2, \cdots$. Hence, if every ϵ_n is let to tend to 0 (in an appropriate way), then, since $s(t) = 0$ when t is an end-point of an I_n, it is seen that $s(t) \to 0$ holds when t tends to ∞ on L. Since $s(t) = 0$ on the complementary set K, this means that $s(\infty)$ exists and is 0.

There remains to be considered the general case (15), where neither (13) nor (16) is assumed. But this case can be reduced to the treatment of the preceding two cases, if the device of splitting the t-axis into an open set L and a closed set K is now chosen as follows: t is in L or in K according as $ds(t)/dt > 0$ or $ds(t)/dt \leqq 0$. The assertion of (ii*) then follows.

The definition of the "confluent" type (D bis) (formulated after the definition of type (D) above) requires that $s(\infty)$ or $\lim |x(t)|$ should not only exist (as a finite limit which may be positive or 0) but should be 0, for every solution $x(t)$ of (1). A corresponding criterion is supplied by the following modification of the preceding (B*)-criterion (ii*):

(ii* bis) *Let* $f(t,x)$ *be continuous on* $H \times R$ *and suppose that*

$$x \cdot f(t,x) \leqq -\lambda(t)\,|\,x\,|^2 \text{ on } H_0 \times R, \tag{18}$$

where $\lambda(t)$ *is a positive continuous function (on* H_0*) satisfying*

$$\int_1^\infty \lambda(t)\,dt = \infty. \tag{19}$$

Then (1) *is of type* (D bis).

Remark. Corresponding to (ii*) *and* to the Remark made after (ii*), the assumption (18) of (ii*) can be relaxed in various directions (cf. also [13], pp. 557-558).

In order to prove (ii* bis), note that (18) implies (13) and so, in view of (ii*), the (B*)-character of (1). This means that, even if (19) is not assumed, all solutions $x(t)$ of (1) exist for $0 \leqq t < \infty$ and lead to a finite limit $x(\infty) \geqq 0$. The assertion of (ii* bis) is that $s(\infty) > 0$ is impossible if (19) is assumed. But it is clear from (1) and (18) that

$$ds(t)/dt \leqq -\lambda(t)s(t), \tag{20}$$

where $s \geqq 0$, $\lambda > 0$ (or just $\lambda \geqq 0$) and $0 \leqq t < \infty$. If (20) is treated in the same way as (17) was treated above, then the assumption $s(\infty) \neq 0$ leads to a contradiction with (19).

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

PART I.

[1] L. Bieberbach, *Theorie der gewöhnlichen Differentialgleichungen auf funktionentheoretischer Grundlage,* Berlin-Goettingen-Heidelberg, 1953.

[2] M. Bôcher, "On regular singular points of linear differential equations of the second order whose coefficients are not necessarily analytic," *Transactions of the American Mathematical Society,* vol. 1 (1900), pp. 40-52.

[3] C. R. Putnam and A. Wintner, "Linear differential equations with almost periodic or Laplace transform coefficients," *American Journal of Mathematics,* vol. 73 (1951), pp. 792-806.

[4] A. Wintner, *Spektraltheorie der unendlichen Matrizen,* Leipzig, 1929.

[5] ———, "On almost free linear motions," *American Journal of Mathematics,* vol. 71 (1949), pp. 595-602.

[6] ———, "On linear asymptotic equilibria," *ibid.,* pp. 853-858.

[7] ———, "On the existence of Laplace solutions for linear differential equations of second order," *ibid.,* vol. 72 (1950), pp. 442-450.

[8] ———, "On the small divisors in integrations by Laplace transforms," *ibid.,* vol. 73 (1951), pp. 173-180.

PART II.

[9] E. A. Coddington and A. Wintner, "On the classical existence theorem of analytic differential equations," *American Journal of Mathematics,* vol. 71 (1949), pp. 886-892.

[10] A. Wintner, "Asymptotic equilibria," *ibid.,* vol. 68 (1946), pp. 125-132.

[11] ———, "The infinities in the non-local existence problem of ordinary differential equations," *ibid.,* vol. 68 (1946), pp. 173-178.

[12] ———, "An Abelian lemma concerning asymptotic equilibria," *ibid.,* vol. 68 (1946), pp. 451-454.

[13] ———, "Asymptotic integration constants," *ibid.,* vol. 68 (1946), pp. 553-559.

[14] ———, "Vortices and nodes," *ibid.,* vol. 69 (1947), pp. 815-824; cf. also "Asymptotic integration constants in the singularity of Briot-Bouquet," *ibid.,* vol. 68 (1946), pp. 293-300.

APPENDIX.

[15] E. Kamke, *Differentialgleichungen reeller Funktionen,* Leipzig, 1930.

[16] P. Painlevé, *Leçons sur la théorie analytique des équations différentielles professées à Stockholm* (1895), Paris, 1897.

[17] K. Weierstrass, "Zur Biographie von," (by G. Mittag-Leffler), *Acta Mathematica,* vol. 35 (1912), pp. 29-65.

[18] A. Wintner, "Unrestricted Riccatian solution fields," *Quarterly Journal of Mathematics* (Oxford series), vol. 18 (1947), pp. 65-71.

[19] ———, "On criteria of linear stability," *Journal of Mathematics and Mechanics,* 1957 (to appear).

MAXIMAL SUBALGEBRAS OF $C(\Gamma)$.*

By KENNETH HOFFMAN and I. M. SINGER.[1]

1. Introduction. In [2], Arens and Singer have presented a generalization of part of the theory of analytic functions in the unit disc, established by observing the role played in the classical theory by the group of integers (and the non-negative portion thereof) and replacing this group by a locally compact abelian group G possessing a suitably distingushed semigroup G_+.

We present here a study of the extension to this context of the following result, established by Wermer [3].

THEOREM 1.1. *Let* $\mathfrak{A}$ *be the Banach algebra of continuous functions on the unit circle,* $|z|=1$, *which can be extended to the unit disc* $|z|\leqq 1$ *so as to be analytic in the interior. The norm is the uniform norm on* $|z|=1$. *Then* $\mathfrak{A}$ *is a maximal subalgebra of the Banach algebra* C *of all continuous complex-valued functions on the unit circle.*

Specifically, we shall show that if, in the Arens-Singer context, G is a discrete abelian group with a semigroup G_+ satisfying the conditions

(1.21) $\qquad G_+ \cup G_+^{-1} = G$; G_+ is a maximal semigroup in G,

the Wermer result is valid if and only if G is archimedean-linearly ordered and G_+ is the set of elements not less than the identity. If the algebra of "analytic" functions is not maximal, we describe completely a maximal subalgebra of C which contains it. A by-product of this investigation is a very brief proof of Theorem 1.1 (see Section 5).

2. Generalized analytic functions. We describe briefly in this section the results of [2] which are pertinent to the present study.

Let G be a discrete abelian group containing a semigroup G_+ such that $G_+ \cup G_+^{-1} = G$. Let A_1 be the Banach algebra of summable functions on G which vanish outside G_+, using the multiplication and the norm defined by

$$(f * g)(x) = \int_{G_+} f(x-y)g(y)\,dy \text{ and } \|f\|_1 = \int_{G_+} |f(x)|\,dx.$$

---

* Received October 26, 1956.

[1] The second named author was supported in part by a National Science Foundation grant during the period of this research.

Let Δ be the set of all multiplicative mappings of the semigroup G_+ into the unit disc of the complex plane. There is a one-one correspondence between the elements ζ in Δ and the homomorphisms h of the Banach algebra A_1 onto the complex numbers, defined by $h(f) = \int_{G_+} f(x)\zeta(x)\,dx$. Through this correspondence we give to Δ the standard topology of the space of complex homomorphisms (regular maximal ideals) of A_1. This topology is identical with the topology of pointwise convergence of elements of Δ as functions on G_+, and is compact Hausdorff.

Each character of the group G defines a multiplicative functional on G_+, and distinct characters of G define distinct functionals since $G_+ \cup G_+^{-1} = G$. This embedding of characters in Δ is a homeomorphism of the character group Γ with a closed subset of Δ.

The canonical Gelfand representation of the Banach algebra A_1 makes correspond to each f in A_1 a continuous function f^T on Δ defined by $f^T(\zeta) = \int_{G_+} f(x)\zeta(x)\,dx$. The mapping of f into f^T is an isomorphism of A_1 with an algebra $A_1{}^T$ of continuous functions on Δ.

In the classical situation, when G is the additive group of integers and G_+ is the semigroup of non-negative integers, the space Δ is the unit disc of the complex plane and Γ is the unit circle. The representing functions f^T are those functions continuous on Δ, analytic in the interior, with an absolutely summable sequence of Taylor coefficients.

Each ζ in Δ has a "polar decomposition" $\zeta = \rho\alpha$, where α is in Γ and ρ is a non-negative functional in Δ. The functional ρ is unique; however, α is not generally unique (though it is if ζ has no zeroes on G_+).

The character group Γ is the Silov boundary of the space Δ of maximal ideals of A_1. That is, Γ is the unique minimal closed subset of Δ on which all the representing functions f^T assume their maximum moduli. Thus, in accordance with a general principle of Arens and Singer [1], there corresponds to each point ζ in Δ a regular Baire measure m_ζ on the boundary Γ, such that for any f in A_1,

$$f^T(\zeta) = \int_\Gamma f^T(\alpha)\,m_\zeta(d\alpha). \tag{2.41}$$

The measure m_ζ generalize (via 2.41) the familiar Poisson integral formula of the classical situation.

A complex-valued function g on Δ is called analytic on Δ if g can be uniformly approximated on Δ by functions f^T with f in A_1. A function is called analytic in the interior of Δ, i. e., $\Delta - \Gamma$, if it can be uniformly approximated on compact subsets of $\Delta - \Gamma$ by functions f^T, f in A_1. Thus, each f^T is analytic; and, in particular, each element x of the semigroup G_+ defines an analytic function x^T on Δ by

$$x^T(\zeta) = \zeta(x). \tag{2.51}$$

We shall at times wish to think of x^T restricted to Γ, that is, consider the character of Γ which x defines. To avoid confusion, we shall therefore call χ_x the character of Γ which an x in G defines, so that

$$\chi_x(\alpha) = \alpha(x) = \langle x, \alpha \rangle. \tag{2.52}$$

3. **Subalgebras.** If C is a (commutative) Banach algebra and A is a subalgebra of C, we call A a *maximal subalgebra* of C if $A \neq C$ and if, for any subalgebra B of C for which $A \subset B \subset C$, either $A = B$ or $B = C$.

If A is any subalgebra of a Banach algebra B (with unit), there is a natural continuous mapping of the space $\mathcal{S}_B$, of complex homomorphisms of B, into the space $\mathcal{S}_A$. This mapping is defined by simply restricting a homomorphism of B to the subalgebra A. The mapping is in general not one-one. We point out that if h is a homomorphism of B and ϕ is an element of A, we may speak of the vaule of the representing function ϕ^T at the point h as $\phi^T(h)$, without any confusion. For, the value of ϕ^T at h is the same whether ϕ is viewed as an element of A or an element of B.

We are interested here in subalgebras of the Banach algebra $C(\Gamma)$ of all continuous complex-valued functions on a compact Hausdorff space Γ. The norm is the uniform norm. If A is a subalgebra of $C(\Gamma)$, there is a continuous mapping of Γ into the space $\mathcal{S}_A$. This mapping sends a point α in Γ into the homomorphism h_α defined by $h_\alpha(f) = f(\alpha)$, $f \in A$. The image of Γ under this mapping is a closed subset of $\mathcal{S}_A$ which obviously includes Ω, the Silov boundary of $\mathcal{S}_A$.

If h_0 is a complex homomorphism of A, then [1; 7.1], there is a regular Baire measure ν_0 on Ω such that $h_0(f) = \int_\Omega f^T(\omega)\nu_0(d\omega)$. Now ν_0 induces, via the mapping of Γ into $\mathcal{S}_A$, a measure μ_0 on Γ such that

$$h_0(f) = \int_\Gamma f(\alpha)\mu_0(d\alpha), \qquad f \in A. \tag{3.11}$$

We have used the fact that $f^T(h_\alpha) = f(\alpha)$.

3.2 THEOREM. *Let A be a subalgebra of $C(\Gamma)$ such that the closed linear space spanned by the functions in A and their complex conjugates is* *all of $C(\Gamma)$. Let B be a subalgebra of $C(\Gamma)$ containing A. If a complex homomorphism h_0 of A is given by the measure μ_0 on Γ (3.11), and if h_0 extends to a homomorphism of B, then h_0 extends uniquely to the element h of $\mathcal{S}_B$ defined by*

$$h(f) = \int_\Gamma f(\alpha)\mu_0(d\alpha), \qquad f \in B. \tag{3.21}$$

Consequently, $\mathcal{S}_B$ is homeomorphic to the closed subset of $\mathcal{S}_A$ of those homomorphisms h_0 (3.11) for which h (3.21) is a multiplicative functional on B.

Proof. If h_0 extends to a multiplicative functional h on B, then h is of the form $h(f) = \int_\Gamma f(\alpha)\mu(d\alpha)$, $f \in B$ for some measure μ on Γ. Since the functions in A, together with their conjugates, span $C(\Gamma)$, a positive functional on $C(\Gamma)$ is completely determined by its effect on the functions in A. Since μ, as a functional on $C(\Gamma)$, agrees with μ_0 on A, we must have $\mu = \mu_0$, i.e., h must be of the form (3.21).

Thus, the natural continuous mapping of $\mathcal{S}_B$ into $\mathcal{S}_A$ is one-one, and because $\mathcal{S}_B$ is compact Hausdorff, the mapping is a homeomorphism of $\mathcal{S}_B$ with its image in $\mathcal{S}_A$.

4. The maximality theorem. Returning to the setting of Section 2, let $\mathfrak{A}$ be the Banach algebra of continuous functions on the boundary Γ which can be extended analytically to the interior of Δ. That is, $\mathfrak{A}$ is the completion under the uniform norm of the algebra of functions obtained by restricting functions in $A_1{}^T$ to the character group Γ.

4.1 THEOREM. *For the continuous function f on Γ to belong to $\mathfrak{A}$, it is necessary and sufficient that*

$$\int_\Gamma \overline{\langle x, \alpha\rangle} g(\alpha)\,d\alpha = 0 \tag{4.11}$$

for each x in G which is not in G_+.

Proof. The necessity is evident from the fact that the property is possessed by functions in $A_1{}^T$. Suppose f has the stated property. For each $\epsilon > 0$ there is a continuous function ϕ on Γ such that $\| f - f * \phi \|_\infty < \epsilon$. By the Plancherel theorem, the Fourier transform of $f * \phi$ is a function F in $L_1(G)$, and the Fourier transform of F is $f * \phi$. But since the Fourier transform of f vanishes off G_+, we see that F is in $L_1(G_+) = A_1$. Thus f can be uniformly approximated on Γ by functions F^T with F in A_1. Consequently, f is in $\mathfrak{A}$.

We now ask when $\mathfrak{A}$ is a maximal subalgebra of $C(\Gamma)$. Clearly, it is necessary that G_+ be a maximal semigroup in G, for any larger (proper) semigroup would immediately yield an algebra properly between $\mathfrak{A}$ and $C(\Gamma)$, e.g., the functions in $C(\Gamma)$ "analytic" with respect to this larger semigroup. However, the maximality of G_+ is not sufficient for the maximality of $\mathfrak{A}$, as we shall soon show.

First, let us make a few observations under the assumptions (1.21). Let

$$G_+ = G_0 \cup G_1, \tag{4.21}$$

where G_0 is the subgroup of G consisting of the elements of G_+ having their inverses in G_+. We distinguish the functional ρ_0 in Δ defined by

$$\rho_0(x) = 1, \quad x \in G_0, \qquad \rho_0 = 0, \quad x \in G_1. \tag{4.22}$$

If we consider the quotient group

$$\mathfrak{G} = G/G_0, \tag{4.23}$$

it is easy to see that

$$\mathfrak{G}_+ = G_+/G_0 \tag{4.24}$$

is a sub-semigroup of this group. The character group of $\mathfrak{G}$ is (of course) isomorphic and homeomorphic to the closed subgroup Λ of Γ which consists of the characters of G which are identically 1 on G_0.

We shall now assemble some useful facts concerning $\mathfrak{G}$, $\mathfrak{G}_+$, ρ_0, etc.

4.3 Lemma. *Under the conditions* (1.21),

i) *the semigroup $\mathfrak{G}_+$ defines an archimedean-linear order on the group $\mathfrak{G}$*

ii) *if x is in G_1* (4.21), *the analytic function x^T* (2.51) *has zeros on Δ exactly at the points $\zeta = \rho_0\alpha$, α in Γ*

iii) *the measure μ_0 on Γ associated with ρ_0 by* (2.41) *is the Haar measure of the subgroup Λ*, i.e., *$\mu_0(E) = \mu(E \cap \Lambda)$ for a Borel set E in Γ, where μ is the Haar measure of the compact group Λ.*

Proof. i) From the definition of G_0, we see that the semigroup $\mathfrak{G}_+$ has only the identity element of $\mathfrak{G}$ in common with $\mathfrak{G}_+^{-1}$. Consequently, $\mathfrak{G}$ is totally (linearly) ordered by the semigroup $\mathfrak{G}_+$. Since G_+ is a maximal semigroup in G, $\mathfrak{G}_+$ is a maximal semigroup in $\mathfrak{G}$. Let ξ and η be elements of $\mathfrak{G}_+$, both different from the identity of $\mathfrak{G}$. Then there must be a positive integer n such that $\xi^n > \eta$, i.e., such that $\xi^n\eta^{-1}$ is in $\mathfrak{G}_+$. For, if this is not the case, the set of elements $\xi^{-n}\theta$, θ in $\mathfrak{G}_+$, is a semigroup properly larger than $\mathfrak{G}_+$ (since ξ^{-1} has been adjoined) and is not all of $\mathfrak{G}$, since $\xi^{-n}\theta > \eta^{-1}$

for every θ in $\mathfrak{G}_+$. Hence, $\mathfrak{G}_+$ defines an archimedean-linear order on $\mathfrak{G}$, with $\mathfrak{G}_+$ the set of elements not less than the identity. ii) If x is in G_1, then $x^T(\rho_0\alpha) = \rho_0(x)\alpha(x) = 0 \cdot \alpha(x) = 0$. Conversely, suppose that $x^T(\rho\alpha) = 0$. Since G_0 is a group, ρ must be identically 1 on G_0. Hence, ρ defines a multiplicative mapping ρ_1 of $\mathfrak{G}_+$ into the unit interval. If η is the coset of x (modulo G_0), then $\rho_1(\eta) = \rho(x) = 0$. If ξ is any element of $\mathfrak{G}_+$ other than the identity, there is a positive integer n such that $\xi^n\eta^{-1}$ is in $\mathfrak{G}_+$. Then

$$\rho_1(\xi)^n = \rho_1(\xi^n) = \rho_1(\eta)\rho_1(\eta^{-1}\xi^n) = 0.$$

Thus ρ_1 is the functional which is 1 at the identity of $\mathfrak{G}$ and is 0 at all other elements of $\mathfrak{G}_+$. Consequently, ρ must be 1 on G_0 and 0 on the remainder of G_+, i.e., $\rho = \rho_0$. iii) The measure μ_0 has the Fourier-Stieltjes transform

$$\mu_0{}^T(x) = \int_\Gamma \overline{\langle x, \alpha\rangle}\mu_0(d\alpha) = 1 \text{ if } x \in G_0, \text{ and } = 0 \text{ if } x \in G - G_0.$$

On the other hand, if μ is Haar measure on Λ,

$$\int_\Lambda \overline{\langle x, \alpha\rangle}\mu(d\alpha) = 1 \text{ if } x \in G_0, \text{ and } = 0 \text{ if } x \in G - G_0.$$

Since a measure on Γ is completely determined by its Fourier-Stieltjes coefficients, we must have $\mu_0(E) = \mu(E \cap \Lambda)$ for each Borel set E.

We now define our candidate for a maximal subalgebra of $C(\Gamma)$ containing $\mathfrak{A}$. Let $\mathfrak{A}_0$ be the subalgebra of $C(\Gamma)$ of those functions f for which

$$\int_\Gamma \overline{\langle x, \alpha\rangle} f(\alpha)\mu_0(d\alpha) = 0, \qquad x \notin G_+.$$

In other words, $\mathfrak{A}_0$ is the collection of continuous functions on Γ whose restrictions to Λ have Fourier transforms that vanish outside the semigroup $\mathfrak{G}_+$ (4.24). When $\mathfrak{A}_0$ is described in this way, one can see easily that $\mathfrak{A}_0$ is an algebra, as we have asserted.

4.5 LEMMA. *$\mathfrak{A}$ is a subalgebra of $\mathfrak{A}_0$.*

Proof. Suppose f is in $\mathfrak{A}$. Then for any x in $G - G_+$,

$$(4.51) \qquad \int \overline{\langle x, \alpha\rangle} f(\alpha)\mu_0(d\alpha) = \int_\Gamma \langle x^{-1}, \alpha\rangle f(\alpha)\mu_0(d\alpha).$$

The first condition of (1.21) tells us that x^{-1} is in G_-. Then, by (2.41) the right integral of (4.51) is

$$(x^{-1})^T(\rho_0)\int_\Gamma f(\alpha)\mu_0(d\alpha)=\rho_0(x^{-1})\int_\Gamma f(\alpha)\mu_0(d\alpha)=0$$

Thus f belongs to $\mathfrak{A}_0$.

4.6 THEOREM. *The space* $\mathcal{S}_{\mathfrak{A}_0}$ *of complex homomorphisms of* $\mathfrak{A}_0$ *is the set of points* ζ *in* Δ *for which either* 1) $\zeta(x)=1$ *for all* x *in* G_0 *or* 2) ζ *is in* Γ.

Proof. Since $\mathfrak{A}\subset\mathfrak{A}_0$, we know from (3.2) that $\mathcal{S}_{\mathfrak{A}_0}$ is homeomorphic to the closed subset of Δ containing the points ζ for which (see (2.41))

$$h(f)=\int_\Gamma f(\alpha)m_\zeta(d\alpha) \tag{4.61}$$

defines a multiplicative functional h on $\mathfrak{A}_0$. Let C_0 denote the algebra of continuous functions on Γ which vanish on Λ. Its space of maximal ideals is $\Gamma-\Lambda$. Furthermore, $C_0\subset\mathfrak{A}_0$. Suppose h (4.61) is multiplicative on $\mathfrak{A}_0$, and let h_0 denote the restriction of h to C_0.

If $h_0\equiv 0$, then the carrier of the measure m_ζ lies in Λ. If $x\in G_0$ and $\alpha\in\Lambda$, then $\langle x,\alpha\rangle=1$, so that

$$1=\int_\Gamma\langle x,\alpha\rangle m_\zeta(d\alpha)=x^T(\zeta)=\zeta(x).$$

Thus 1) holds.

If $h_0\not\equiv 0$, then there exists a point γ in $\Gamma-\Lambda$ such that for every f in C_0

$$\int_\Gamma f(\alpha)m_\zeta(d\alpha)=h(f)=h_0(f)=f(\gamma).$$

Let N be any open set containing γ such that $N\cap\Lambda$ is empty. Let g_N be a non-negative continuous function on Γ which is identically one on $\Gamma-N$ and vanishes at γ. Then $1-g_N$ belongs to C_0 and

$$\int_\Gamma(1-g_N(\alpha))m_\zeta(d\alpha)=1-g_N(\gamma)=1.$$

Since $m_\zeta(\Gamma)=1$, we have $\int_\Gamma g_N(\alpha)m_\zeta(d\alpha)=0$. Therefore the measure m_ζ is concentrated at the point γ. Thus $\zeta=\gamma$ and 2) holds.

If 2) holds, h (4.61) is obviously multiplicative on $\mathfrak{A}_0$. If 1) holds,

ζ defines a multiplicative functional on $\mathcal{G}_+$ (4.24) and hence a homomorphism of $\mathfrak{A}_0/C_0$, thus a homomorphism of $\mathfrak{A}_0$.

Our maximality theorem is as follows.

4.7 THEOREM. *The algebra* $\mathfrak{A}_0$ *is a maximal subalgebra of* $C(\Gamma)$ *containing* $\mathfrak{A}$. *In order that* $\mathfrak{A}$ *be maximal, i.e. that* $\mathfrak{A} = \mathfrak{A}_0$, *it is necessary and sufficient that* G *be archimedean-linearly ordered, with* G_+ *the semigroup of elements not less than the identity.*

Proof. To see that $\mathfrak{A}_0$ is maximal. we assume that $\mathfrak{B}$ is a subalgebra of $C(\Gamma)$ which contains $\mathfrak{A}_0$. We know from (4.6) that ρ_0 (4.22) defines a homomorphism of $\mathfrak{A}_0$. (i) If the ρ_0 homomorphism extends to $\mathfrak{B}$, it does so in the form

$$h(f) = \int_\Gamma f(\alpha)\mu_0(d\alpha). \tag{4.71}$$

Let f be in $\mathfrak{B}$. Then for any x in $G - G_+$,

$$\int_\Gamma \overline{\langle x, \alpha\rangle} f(\alpha)\mu_0(d\alpha) = \int_\Gamma \langle x^{-1}, \alpha\rangle f(\alpha)\mu_0(d\alpha) = \rho_0(x^{-1}) \int_\Gamma f(\alpha)\mu_0(d\alpha).$$

But x^{-1} is an element of G_+ not in G_0, so that $\rho_0(x^{-1}) = 0$. Consequently, for x in $G - G_+$,

$$\int_\Gamma \overline{\langle x, \alpha\rangle} f(\alpha)\mu_0(d\alpha) = 0.$$

Thus, f is in $\mathfrak{A}_0$. Therefore $\mathfrak{B} = \mathfrak{A}_0$. (ii) If the ρ_0 homomorphism (4.71) does not extend to $\mathfrak{B}$, we shall show that $\mathfrak{B} = C(\Gamma)$. Let x be an element of $G_1 = G_+ - G_0$. From part (ii) of (4.3) we know that the only zeros of x^T on Δ are at the points $\zeta = \rho_0\alpha$, α in Γ. On the other hand, (4.6) tells us that the only such point in $\mathcal{S}_{\mathfrak{A}_0}$ is ρ_0. Consequently, viewing χ_x (2.52) as an element of $\mathfrak{B}$, we see that its representing function has no zeros on $\mathcal{S}_{\mathfrak{B}}$ (ρ_0 having been removed). Therefore $\chi_x^{-1} = \chi_{x^{-1}}$ is in $\mathfrak{B}$. Thus $\mathfrak{B}$ contains all characters of Γ and must be all of $C(\Gamma)$.

The condition that $\mathfrak{A} = \mathfrak{A}_0$ is evidently that the subgroup Λ be all of Γ; for, if this is not the case, $\mathfrak{A}$ must be properly included in $\mathfrak{A}_0$ because $\mathfrak{A}_0$ contains all functions in $C(\Gamma)$ which vanish on Λ. But, the condition that $\Lambda = \Gamma$ is simply the condition that G_0 reduces to the identity, i.e., that G is isomorphic to the archimedean-linearly ordered group $\mathcal{G}$ (see 4.3, part (i)).

An interesting example of the situation which this theorem describes is obtained by letting G be the additive group of the Gaussian integers, that is, the direct sum of the group of integers with itself. The most natural semigroup to consider is the pairs of integers (m, n) for which $m \geqq 0$, $n \geqq 0$. However, this semigroup does not satisfy $G_+ \cup G_+^{-1} = G$. This can be remedied by adding to the set the pairs (m, n) with $m < 0$ and $n > 0$. Now we have a semigroup satisfying the first condition of (1.21). However, this is not a maximal semigroup, so we extend it to the set G_+ of pairs (m, n) for which $n \geqq 0$, m arbitrary. Then G_+ is a maximal semigroup. The character group Γ is then the torus; the subgroup G_0 of G is the set of pairs $(m, 0)$; the subgroup Λ of Γ is a unit circle on the torus, in fact, $\Gamma = \Lambda \times \Lambda$. The algebra $\mathfrak{A}$ consists of the continuous functions f on the torus such that, for every integer m, the function g_m on the unit circle defined by $g_m(\theta) = \int_0^{2\pi} f(\psi, \theta) e^{im\psi} d\psi$ has a Fourier transform vanishing on the negative integers. The maximal subalgebra $\mathfrak{A}_0$ is the collection of continuous functions f for which the function $g(\theta) = f(0, \theta)$ is an "analytic" function on the unit circle.

5. The classical case. It would seem worthwhile at this point to see how these methods apply to the classical situation, in order that the simplicity of the argument in that case should not be lost in the complexities of the more general situation. The argument which we present applies with virtually no change to all cases where G is archimedean-linearly ordered (subgroup of the additive group of real numbers) and G_+ is the semigroup of non-negative elements.

Proof of Theorem 1.1. Suppose that $\mathfrak{B}$ is a subalgebra of C which contains $\mathfrak{A}$. The origin, $z = 0$, defines a homomorphism h of $\mathfrak{A}$ by

$$h(f) = \frac{1}{2\pi} \int_0^{2\pi} f(e^{i\theta}) d\theta. \tag{5.11}$$

(i) Suppose that the homomorphism (5.11) extends to $\mathfrak{B}$. This homomorphism is represented by a measure μ on $|z| = 1$, and since any measure on the unit circle is completely determined by the Fourier-Stieltjes coefficients $\frac{1}{2\pi} \int_0^{2\pi} e^{in\theta} \mu(d\theta)$, $n = 0, 1, 2, \cdots$, the measure μ must be (normalized) Lebesgue measure. Consequently, for any f in $\mathfrak{B}$ and any positive integer n,

$$\frac{1}{2\pi} \int_0^{2\pi} e^{in\theta} f(e^{i\theta}) d\theta = z^n(0) \cdot \frac{1}{2\pi} \int_0^{2\pi} f(e^{i\theta}) d\theta = 0.$$

Thus, the Fourier transform of f vanishes on the negative integers, i.e., f belongs to $\mathfrak{A}$. (ii) If the homomorphism (5.11) does not extend to $\mathfrak{B}$, the functions $\chi_n(\theta) = e^{in\theta}$, $n = 1, 2, \cdots$ belong to no maximal ideal of $\mathfrak{B}$, as the analytic functions z^n vanish only at $z = 0$. Consequently, each χ_n is invertible in $\mathfrak{B}$. Therefore, $\mathfrak{B}$ contains all characters χ_n, $n = 0, \pm 1, \pm 2, \cdots$, so that $\mathfrak{B} = C$.

6. Concluding remarks. The method of this paper is a special case of a general procedure for finding maximal subalgebras $\mathfrak{A}_0$ of $C(X)$ which separate the points of X. If $\mathfrak{A}$ is a "separating" subalgebra of $C(X)$, then its space of maximal ideals $\mathscr{M}_{\mathfrak{A}}$ contains X. Since the norm of a function in $\mathfrak{A}$ is its sup over X, X contains the Silov boundary Γ of $\mathfrak{A}$. Let Λ be a closed subset of X and let $\mathfrak{A}_\Lambda$ denote the closure of the restriction of functions in $\mathfrak{A}$ to the set Λ, so that $\mathfrak{A}_\Lambda$ is a subalgebra of $C(\Lambda)$. Let $\mathfrak{A}_0$ be the subalgebra of $C(X)$ consisting of all continuous functions on X whose restriction to Λ lies in $\mathfrak{A}_\Lambda$. $\mathfrak{A} \subset \mathfrak{A}_0$; and if $\mathfrak{A}_\Lambda \neq C(\Lambda)$, then $\mathfrak{A}_0 \neq C(X)$. Thus $\mathfrak{A}$ cannot be a maximal subalgebra if $\mathfrak{A}_\Lambda \neq C(\Lambda)$ and $\mathfrak{A} \neq \mathfrak{A}_0$. This is the situation in the non-archimedean ordered case of Section 4, where we go on to prove that $\mathfrak{A}_0$ is maximal because $\mathfrak{A}_\Lambda$ is maximal in $C(\Lambda)$. Thus the maximal subalgebras $\mathfrak{A}$ of $C(X)$ are of two kinds. Of the first type are those for which there exists a closed subset Λ such that $\mathfrak{A}_\Lambda$ is maximal in $C(\Lambda)$ and $\mathfrak{A} = \mathfrak{A}_0$ [though it is not clear that all such algebras are maximal]; of the second type are those for which no such subset exists. For the first type, the problem "reduces" to finding the maximal subalgebras of $C(\Lambda)$.

Note further that in order for $\mathfrak{A}$ to be maximal in $C(X)$, the Silov boundary $\Gamma = X$. For the map: $f \to f|\Gamma$ is norm preserving and therefore gives an isomorphism of $\mathfrak{A}$ with $\mathfrak{A}_\Gamma$. If $\mathfrak{A}_\Gamma = C(\Gamma)$, then $\Gamma = \mathscr{M}_{\mathfrak{A}_\Gamma} = \mathscr{M}_{\mathfrak{A}} \supset X$, so that $\Gamma = X$. If $\mathfrak{A}_\Gamma \neq C((\Gamma))$, then $\mathfrak{A}_0 = \mathfrak{A}$ (by maximality of $\mathfrak{A}$) so that every function in $\mathfrak{A}_0$ has a unique extension to X. In particular, the zero function on Γ has a unique extension to X, i.e., $\Gamma = X$.

So in seeking maximal subalgebras we can assume the Silov boundary is X. Suppose $\mathscr{M}_{\mathfrak{A}} \neq X$. Consider the class $\mathscr{C}$ of subalgebras of $C(X)$ with the same space of maximal ideals $\mathscr{M}_{\mathfrak{A}}$. Let $\mathfrak{A}_\alpha$ be an increasing family (under inclusion) of algebras in $\mathscr{C}$. Let $\mathfrak{B}$ be the closure of the algebra $\bigcup_\alpha \mathfrak{A}_\alpha$. One can easily check that $\mathfrak{B} \in \mathscr{C}$. Consequently, Zorn's lemma applies and we conclude that every $\mathfrak{A} \in \mathscr{C}$ is contained in a maximal $\mathfrak{B} \in \mathscr{C}$. Since $\mathscr{M}_{\mathfrak{B}} = \mathscr{M}_{\mathfrak{A}} \neq X$, $\mathfrak{B} \neq C(X)$. Therefore, in order for $\mathfrak{A}$ to be maximal in $C(X)$, then $\mathfrak{A}$ must be maximal in $\mathscr{C}$.

Suppose, then, that $\mathfrak{A}$ is maximal in $\mathscr{C}$ and $\mathfrak{A} \subsetneqq \mathfrak{B} \subset C(X)$. Then $\mathscr{M}_{\mathfrak{B}} \neq \mathscr{M}_{\mathfrak{A}}$ and by Theorem 3.2 (under the conditions of this theorem)

$\mathcal{S}_{\mathfrak{B}} \underset{\neq}{\subset} \mathcal{S}_{\mathfrak{A}}$. The problem now is to show that there are sufficiently many functions $\{f_\alpha\}$ in $\mathfrak{A}$ whose zeros lie entirely in $\mathcal{S}_{\mathfrak{A}} - \mathcal{S}_{\mathfrak{B}}$ $(f_\alpha^{-1} \in \mathfrak{B})$, such that $\mathfrak{A}$, $\{f_\alpha\}$ generate all of $C(X)$, i.e., $\mathfrak{B} = C(X)$. The proof of the main theorem is the verification that $\mathfrak{A}$ is maximal in $\mathcal{C}$ and enough such functions f_α exist.

It was pointed out to us by Wermer and de Leeuw that the sup norm is not essential to these arguments.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY.

REFERENCES.

[1] Richard Arens and I. M. Singer, "Function values as boundary integrals," *Proceedings of the American Mathematical Society*, vol. 5 (1954), pp. 735-745.

[2] Richard Arens and I. M. Singer, "Generalized analytic functions," *Transactions of the American Mathematical Society*, vol. 81 (1956), pp. 379-393.

[3] John Wermer, "On algebras of continuous functions," *Proceedings of the American Mathematical Society*, vol. 4 (1953), pp. 866-869.

ON THE TOTAL CURVATURE OF IMMERSED MANIFOLDS.*

By SHIING-SHEN CHERN[1] and RICHARD K. LASHOF.

Introduction. In the classical theory of surfaces in the ordinary Euclidean space E an important rôle is played by the normal mapping of Gauss: Let M be an oriented surface which has at every point x a well-defined unit normal vector $\nu(x)$. Then the normal mapping $\nu : M \to S_0$ is the mapping of M into the unit sphere S_0 about the origin of E, which sends x to $\nu(x)$.

For differentiably immersed submanifolds in an Euclidean space of higher dimension the following is a generalization of the Gauss mapping: We consider a C^∞-manifold M^n of dimension n, and a C^∞-mapping $x : M^n \to E^{n+N}$ into the Euclidean spase E^{n-N} of dimension $n+N$ $(N \geqq 1)$. M^n, or rather M^n and the mapping x, is called an immersed submanifold, if the induced mapping of the tangent space is univalent everywhere, or, what is the same, if the Jacobian matrix of x is everywhere of rank n. The submanifold M^n is said to be imbedded, if x is one-one; that is, if $x(p) = x(q)$, $p, q \in M^n$, implies that $p = q$. Let B_ν be the bundle of unit normal vectors of $x(M^n)$, so that a point of B_ν is a pair $(p, \nu(p))$, where $\nu(p)$ is a unit normal vector to $x(M^n)$ at $x(p)$. Then B_ν is a bundle of $(N-1)$ dimensional spheres over M^n and is a C^∞-manifold of dimension $n+N-1$. The mapping $\nu : B_\nu \to S_0^{n+N-1}$ of B_ν into the unit sphere S_0^{n+N-1} of E^{n+N} defined by $\tilde{\nu}(p, \nu(p)) = \nu(p)$ is the mapping with which we will be concerned in this paper.

Let dV be the volume element of M^n. There is a differential form $d\sigma_{N-1}$ of degree $N-1$ on B_ν such that its restriction to a fiber is the volume element of the sphere of unit normal vectors at a point $p \in M^n$; then $d\sigma_{N-1} \wedge dV$ is the volume element of B_ν (for detail see Section 2). Let $d\Sigma_{n+N-1}$ be the volume element of S_0^{n+N-1}. The function $G(p, \nu(p)) = G(p, \nu)$ defined by

$$\tilde{\nu}^* d\Sigma_{n+N-1} = G(p, \nu)\, d\sigma_{N-1} \wedge dV, \tag{1}$$

where $\tilde{\nu}^*$ is the dual mapping on differential forms induced by $\tilde{\nu}$, is a function in B_ν. It generalizes the Gauss-Kronecker curvature and we will call

---

* Received January 4, 1957.

[1] Work done when the first-named author is under partial support from a contract with the National Science Foundation.

it the Lipschitz-Killing curvature at $\nu(p)$. $G(p,\nu)$ has a geometrical interpretation which we will discuss below. It is zero at a point $(p,\nu(p)) \in B_\nu$, if and only if $\bar{\nu}$ has a critical value at this point. We call the integral

$$K^*(p) = \int |G(p,\nu)|\, d\sigma_{N-1} \geqq 0 \tag{2}$$

over the sphere of unit normal vectors at $x(p)$ the *total curvature of* M^n *at* p, and define as the *total curvature of* M^n itself the integral $\int_{M^n} K^*(p)\,dV$, if it converges.

The main results of this paper are concerned with the conclusions on M^n when its total curvature is "small." They can be stated as the following theorems:

THEOREM 1. *Let* M^n *be a compact oriented* C^∞*-manifold immersed in* E^{n+N}. *Its total curvature satisfies the inequality:*[2]

$$\int_{M^n} K^*(p)\,dV \geqq 2c_{n+N-1} \tag{3}$$

THEOREM 2. *Under the hypothesis of Theorem* 1, *if*

$$\int_{M^n} K^*(p)\,dV < 3c_{n+N-1}, \tag{4}$$

then M^n *is homeomorphic to a sphere of n-dimensions.*

THEOREM 3. *Under the same hypothesis, if*

$$\int_{M^n} K^*(p)\,dV = 2c_{n+N-1}, \tag{5}$$

then M^n *belongs to a linear subvariety* E^{n+1} *of dimension* $n+1$, *and is imbedded as a convex hypersurface in* E^{n+1}. *The converse of this is also true.*

These theorems generalize known results of Fenchel, Fary [2], and Milnor [3] for curves and sharpen some results of Milnor and one of us [1]. Theorem 3 can be interpreted as a characterization of convex hypersurfaces among all immersed submanifolds of a given dimension in an Euclidean space of arbitrary dimension. A large part of our paper is devoted to a proof of this theorem.

1. Moving frames. Suppose E^{n+N} be oriented. By a frame $xe_1 \cdots e_{n+N}$ in E^{n+N} we mean a point x and an ordered set of mutually perpendicular unit vectors $e_1, \cdots, e_{n+N}$, such that their orientation is coherent with that of E^{n+N}. Unless otherwise stated, we agree on the following ranges of the indices:

---

[2] c_{n+N-1} is the area of the unit hypersphere in an Euclidean space of dimension $n+N$.

$$(6) \qquad 1 \leqq i, j, k \leqq n, \quad n+1 \leqq r, s, t \leqq n+N, \quad 1 \leqq A, B, C \leqq n+N.$$

Then we have

$$(7) \qquad e_A e_B = \delta_{AB},$$

where the left-hand side is the scalar product of vectors. Let $F(n, N)$ be the space of all frames in E^{n+N}, so that $\dim F(n, N) = (n+N)(n+N+1)/2$. In $F(n, N)$ we introduce the linear differential forms ω'_A, ω'_{AB} by the equations

$$(8) \qquad de_A = \sum_B \omega'_{AB} e_B, \qquad dx = \sum_A \omega'_A e_A,$$

where

$$(9) \qquad \omega'_{AB} + \omega'_{BA} = 0.$$

Their exterior derivatives satisfy the equation of structure:

$$(10) \qquad d\omega'_A = \sum_B \omega'_B \wedge \omega'_{BA}, \qquad d\omega'_{AB} = \sum_C \omega'_{AC} \wedge \omega'_{CB}.$$

As explained in the Introduction, we mean by an immersed submanifold in E^{n+N} an abstract C^∞-manifold M^n and a C^∞-mapping $x\colon M^n \to E^{n+N}$, such that the induced mapping x_* on the tangent space is everywhere univalent. Analytically, the mapping can be defined by a vector-valued function $x(p)$, $p \in M^n$. Our assumption implies that the differential $dx(p)$ of $x(p)$, which is a linear differential form in M^n, with value in E^{n+N}, has as values a linear combination of n vectors, $t_1, \cdots, t_n$, and not less. Since x_* is univalent, we can identify the tangent space of M^n at p with the vector space spanned by $t_1, \cdots, t_n$. A linear combination of the latter is called a tangent vector and a vector perpendicular to them is called a normal vector. The immersion of M^n in E^{n+N} gives rise to the following fiber bundles over M^n:

1) The tangent bundle B_T, whose bundle space is the subset of $M^n \times E^{n+N}$, consisting of all points (p, v), such that $p \in M$ and v is a unit tangent vector at $x(p)$.

2) The normal bundle B_ν, whose bundle space is the subset of $M^n \times E^{n+N}$, consisting of all points (p, v), such that $p \in M$ and v is a unit normal vector at $x(p)$.

3) The bundle B, whose bundle space is the subset of $M^n \times F(n, N)$, consisting of $(p, x(p) e_1 \cdots e_n e_{n+1} \cdots e_{n+N}) \in M^n \times F(n, N)$ such that $e_1, \cdots, e_n$

are tangent vectors and $e_{n+1}, \cdots, e_{n+N}$ are normal vectors at $x(p)$. The projection $B \to M^n$ we denote by ψ.

The last bundle B is the space in which most of our computations take place.[3] We define the mappings

$$\psi_T : B \to B_T, \qquad \psi_\nu : B \to B_\nu, \tag{11}$$

by

$$\psi_T(p, x(p)e_1 \cdots e_{n+N}) = (p, e_n), \qquad \psi_\nu(p, x(p)e_1 \cdots e_{n+N}) = (p, e_{n+N}). \tag{12}$$

We also remark that the Whitney sum $B_T \oplus B_\nu$ over M^n is equivalent to the product bundle $M^n \times S^{n+N-1} \to M^n$.

Consider the mappings

$$B \xrightarrow{i} M^n \times F(n,N) \xrightarrow{\lambda} F(n,N), \tag{13}$$

where i is inclusion and λ is the projection into the second factor. Put

$$\omega_A = (\lambda i)^* \omega'_A, \qquad \omega_{AB} = (\lambda i)^* \omega'_{AB}, \tag{14}$$

Then we have, from (9) and (10),

$$\omega_{AB} + \omega_{BA} = 0, \tag{15}$$

$$d\omega_A = \sum_B \omega_B \wedge \omega_{BA}, \qquad d\omega_{AB} = \sum_C \omega_{AC} \wedge \omega_{CB}. \tag{16}$$

From our definition of B it follows that $\omega_r = 0$ and that ω_i are linearly independent. Hence the first equation of (16) gives

$$\sum_i \omega_i \wedge \omega_{ir} = 0.$$

From this it follows that

$$\omega_{ir} = \sum_j A_{rij}\omega_j, \qquad A_{rij} = A_{rji}. \tag{17}$$

2. The total curvature. An essential idea of the method of moving frames is to consider the bundle space B, and to construct differential forms in B, which are inverse images of differential forms in M^n and B_ν, under the mappings ψ and ψ_ν respectively. In particular, the volume element of M^n can be written

---

[3] The bundle B can also be defined as follows: Let Q_{n+N} be the group of all orientation-preserving motions in E^{n+N}, and $R_n \times R_N$ the subgroup of Q_{n+N} consisting of all motions which leave fixed the origin 0 of E^{n+N} and a given oriented linear space of dimension n through 0. Then $Q_{n+N} \to Q_{n+N}/R_n \times R_N$ is a bundle whose structure group is $R_n \times R_N$ and whose base space is the space of all elements consisting of a point and an oriented linear space of dimension n through it. The bundle B is induced by the mapping which sends $p \in M$ to the point $x(p)$ and the oriented tangent space at $x(p)$. In particular, the structural group of B is $R_n \times R_N$. Similarly, we can define the bundles B_T and B_ν.

$$(18) \qquad dV = \omega_1 \wedge \cdots \wedge \omega_n,$$

and the volume element of B_ν is

$$(19) \qquad dV \wedge d\sigma_{N-1} = \omega_1 \wedge \cdots \wedge \omega_{n+N,n+1} \wedge \cdots \wedge \omega_{n+N,n+N-1},$$

$d\sigma_{N-1}$ being equal to the product of the last $N-1$ factors. On the other hand, we have

$$\bar{\nu}^* d\Sigma_{n+N-1} = \omega_{n+N,1} \wedge \cdots \wedge \omega_{n+N,n} \wedge \omega_{n+N,n+1} \wedge \cdots \wedge \omega_{n+N,n+N-1}.$$

Using (17), we get

$$\bar{\nu}^* d\Sigma_{n+N-1}$$
$$= (-1)^n \det(A_{n+N,ij}) \omega_1 \wedge \cdots \wedge \omega_n \wedge \omega_{n+N,n+1} \wedge \cdots \wedge \omega_{n+N,n+N-1}.$$

It follows from the definition (1) of the Lipschitz-Killing curvature $G(p,\nu)$ that

$$(20) \qquad G(p,\nu) = (-1)^n \det(A_{n+N,ij}).$$

To see how $G(p,\nu)$ depends on ν, we take a local cross-section of M^n in B, described by the functions $\tilde{e}_A(q)$ for q in a neighborhood of p. Then for any frame $e_A(q)$ in B at $x(q)$, we have $e_A = \sum c_{AB} \tilde{e}_B(q)$ and

$$\sum_{i,j} A_{sij} \omega_i \omega_j = \sum_{r,i,j} c_{sr} \tilde{A}_{rij} \tilde{\omega}_i \tilde{\omega}_j,$$

where $\tilde{A}_{rij}$ is the function A_{rij} restricted to the local cross-section. In particular, if for $\nu = e_{n+N}$ we write $\nu = \sum \nu_r \tilde{e}_r$ we have at p:

$$(21) \qquad G(p,\nu) = (-1)^n \det(\sum_r \nu_r \tilde{A}_{rij}(p)).$$

Further we get for the scalar product of ν and the vector-valued second differential d^2x on B

$$(22) \qquad \nu \cdot d^2x = \sum_{i,r} \nu_r \tilde{\omega}_{ir} \tilde{\omega}_i = \sum_{r,i,j} \nu_r \tilde{A}_{rij} \tilde{\omega}_i \tilde{\omega}_j$$

and hence as forms on B_ν we have:

$$(23) \qquad -d\nu dx = \nu \cdot d^2x = \sum_{r,i,j} \nu_r \tilde{A}_{rij} \tilde{\omega}_i \tilde{\omega}_j.$$

Therefore we may interpret $G(p,\nu)$ as generalizing the determinant of the second fundamental form of a surface.

If $N=1$, i.e., if M^n is an immersed oriented hypersurface in E^{n+1}, its orientation (and that of E^{n+1}) defines a unit normal vector $\nu_0(p)$ at $p \in M^n$. Then $G(p, \nu_0(p)) = G(p)$ is called the Gauss-Kronecker curvature of M at p. Any other unit normal vector at p is of the form $\nu(p) = \pm \nu_0(p)$, and

$$G(p, \nu(p)) = G(p, \pm \nu_0(p)) = (\pm 1)^n G(p).$$

It follows that, for n even, $G(p, \nu(p))$ is independent of the orientation of the hypersurface M^n and of the space E^{n+1}. Naturally, $G(p)$ reduces for $n = 2$ to the classical Gaussian curvature.

In the general case $G(p, \nu)$ admits the following geometrical interpretation in terms of the Gauss-Kronecker curvature: Let $L(\nu)$ be the linear space of dimension $n+1$ spanned by the tangent space to $x(M^n)$ at $x(p)$ and the normal vector $\nu(p)$. Then $G(p, \nu)$ is equal to the Gauss-Kronecker curvature at p of the orthogonal projection of $x(M^n)$ into $L(\nu)$.

Since the theorem is local, we take a local cross-section $\tilde{e}_A(q)$ of M^n in B in a neighborhood of p, such that $\nu(p) = \tilde{e}_{n+N}(p)$. We write

$$\tilde{e}_A(p) = (\tilde{e}_A)_0, \qquad x(p) = x_0.$$

If $x'(q)$ denotes the position vector of the projection of $x(q)$ in $L(\nu)$, $x'(q)$ is defined by the equations

$$x'(q) - x(q) = \xi_{n+1}(\tilde{e}_{n+1})_0 + \cdots + \xi_{n+N-1}(\tilde{e}_{n+N-1})_0,$$

$$x'(q) - x_0 \equiv 0, \qquad \operatorname{mod}(\tilde{e}_1)_0, \cdots, (\tilde{e}_n)_0, (\tilde{e}_{n+N})_0.$$

From this it follows that

$$\xi_{n+\lambda} = (x'(q) - x(q)) \cdot (\tilde{e}_{n+\lambda})_0 = (x_0 - x(q)) \cdot (\tilde{e}_{n+\lambda})_0 \qquad 1 \leqq \lambda \leqq N-1.$$

If p is fixed and q varies on the manifold M^n, we have

$$dx' = dx + \sum_\lambda d\xi_{n+\lambda}(\tilde{e}_{n+\lambda})_0 = dx - \sum_\lambda (dx \cdot (\tilde{e}_{n+\lambda})_0)(\tilde{e}_{n+\lambda})_0,$$

$$d^2x' = d^2x - \sum_\lambda (d^2x \cdot (\tilde{e}_{n+\lambda})_0)(\tilde{e}_{n+\lambda})_0,$$

so that $(\tilde{e}_{n+N})_0 d^2x' = (\tilde{e}_{n+N})_0 d^2x$. This proves our statement.

3. Proof of Theorem 1.

For this proof we will need the following:

THEOREM (Sard)[4] *Let V and W be two C^1-manifolds of the same dimension and f a mapping of class C^1 of V into W. The image $f(E)$ of the set E of critical points of f is a set of measure zero in W.*

---

[4] Cf. [6], p. 10.

We consider the map $\bar{\nu}: B_\nu \to S_0^{n+N-1}$. Every point of S_0^{n+N-1} is covered at least twice by $\bar{\nu}$. In fact, for a fixed unit vector ν_0, the scalar product $\nu_0 \cdot x(p)$ as a continuous function on M^n has at least one maximum and one minimum, at which $\pm \nu_0 dx(p) = 0$. If, on the other hand, the maximum and minimum points are the same then M^n is contained in a hyperplane perpendicular to ν_0, and every point of M^n has ν_0 as a normal vector.

The set of critical points of $\bar{\nu}$ is the set E of points in B_ν such that $G(p,\nu) = 0$. Hence

$$\int_{M^n} K^*(p)\,dV = \int_{B_\nu} |\,G(p,\nu)\,|\,dV d\sigma_{N-1}$$

is the volume of the image in S_0^{n+N-1} of the set of non-critical points of B_ν. By Sard's theorem and by the above remark that every point of S_0^{n+N-1} is covered at least twice by $\bar{\nu}$, we have immediately

$$\int_{M^n} K^*(p)\,dV \geqq 2c_{n+N-1}.$$

4. **Proof of Theorem 2.** Suppose that $\int_{M^n} K^*(p)\,dV < 3c_{n+N-1}$; we wish to show that M^n is homeomorphic to a sphere of n dimensions. Our hypothesis implies that there exists a set of positive measure on S_0^{n+N-1} such that if ν_0 is a unit vector in this set, $\nu_0 \cdot x(p)$ has just two critical points. For if not; every point of S_0^{n+N-1}, except for a set of measure zero, would be covered at least three times by ν and hence as in Section 3 we would have

$$\int_{M^n} K^*(p)\,dV \geqq 3c_{n+N-1}.$$

Since, by Sard's theorem, the image of the set of critical points under $\bar{\nu}$ is of measure zero, there is a unit vector ν_0 such that $\nu_0 \cdot x(p)$ has exactly two critical points on M^n and such that ν_0 is the image of non-critical points of B_ν under $\bar{\nu}$. The latter means that $G(p,\nu_0) \neq 0$ at each critical point $p \in M$ of the function $\nu_0 \cdot x(p)$, which is equivalent to saying that $\nu_0 \cdot d^2x$ is a quadratic differential form of determinant not zero. In other words, the function $\nu_0 \cdot x(p)$ on M^n has exactly two non-degenerate critical points. Now a theorem of Reeb [5] (see also [4], p. 401) asserts that if a compact differentiable manifold M has a real-valued differentiable function on it with only two critical points which are non-degenerate, then M is homeomorphic to a sphere. It follows from this that M^n is homeomorphic to a sphere, and our theorem is proved.

5. Proof of Theorem 3.

We begin with two lemmas:

LEMMA 1. *Under the hypothesis of Theorem 3, M^n is immersed in a linear subvariety of dimension $n+1$ of E^{n+N}.*

We may assume $N \geqq 2$, since otherwise there is nothing to prove. We will first show that M is contained in a hyperplane of E^{n+N}. In doing this, we show that the hypothesis of Theorem 3 and the assumption that M^n does not lie in a hyperplane of E^{n+N} lead to a contradiction.

Let $(p, \nu_0(p)) \in B_\nu$ be such that $G(p, \nu_0) \neq 0$; such a point exists by Theorem 1. Choose a local cross-section of M^n in B; i. e., the vectors $\tilde{e}_A(q)$, where q belongs to a neighborhood of p, and that $\tilde{e}_{n+N}(p) = \nu_0$. Then any other unit normal vector at p may be written $\nu = \sum_r \nu_r \tilde{e}_r(p)$ and by equation (21), Section 3, we have $G(p, \nu) = (-1)^n \det(\sum_r \nu_r \tilde{A}_{rij}(p))$. Holding p fixed and restricting ourselves to normal vectors $\nu(\theta)$ such that

$$\nu_{n+N} = \cos\theta, \quad \nu_{n+N-1} = \sin\theta, \qquad \nu_r = 0, r \neq n+N-1, n+N,$$

we have $G(p, \nu) = f(\theta)$, where $f(\theta)$ is a polynomial in $\cos\theta$ and $\sin\theta$ and is hence an analytic function of θ. $f(\theta)$ is not identically zero, since $f(0) = G(p, \nu_0) \neq 0$.

Let H_θ be the tangent hyperplane at $x(p)$ perpendicular to $\nu = \nu(\theta)$. Since $x(M^n)$ does not belong to a hyperplane, there exist tangent hyperplanes H_{θ_1}, H_{θ_2}, $\theta_1 < \theta_2$, and points $q_1, q_2 \in M$, such that $x(q_1) \in H_{\theta_1}$, $x(q_2) \in H_{\theta_2}$, $x(q_1) \notin H_{\theta_2}$, $x(q_2) \notin H_{\theta_1}$. Since $f(\theta)$ does not vanish identically, there is a tangent hyperplane H_{θ_3}, such that $f(\theta_3) \neq 0$ and that $x(q_1)$ and $x(q_2)$ lie on different sides of the tangent hyperplane H_{θ_3}. The condition $f(\theta_3) \neq 0$ implies that the mapping $\tilde{\nu}$ is one-one in a neighborhood W of $(p, \nu(\theta_3))$ of B_ν. We can choose W so small that for $(q', \nu') \in W$, $x(q_1)$ and $x(q_2)$ lie on different sides of the tangent hyperplane perpendicular to ν' at $x(q')$. The function $\nu' \cdot x$ in M^n has at least three point at which $\nu' \cdot dx = 0$; namely, the maximum, the minimum, and the point q'. The last point q' is distinct from the maximum and the minimum, since, by our construction, there are points of $x(M^n)$ on different sides of the tangent hyperplane at q' perpendicular to ν'. It follows that a neighborhood of S_0^{n+N-1} is covered by the image of $\tilde{\nu}$ at least three times. As every point of S_0^{n+N-1} is covered at least twice, we conclude that the total curvature of $x(M^n)$ is strictly greater than $2c_{n+N-1}$. But this is a contradiction.

It follows from this contradiction that $x(M^n)$ belongs to a hyperplane E^{n+N-1} of E^{n+N}. We wish to show that its total curvature in E^{n+N-1} is equal to $2c_{n+N-2}$. We denote by v the unit vector perpendicular to E^{n+N-1} and by S_0^{n+N-2} the unit sphere in E^{n+N-1}. The sphere S_0^{n+N-2} can be imagined as the equator of S^{n+N-1} with v as the north pole. Let B_ν' be the bundle of unit normal vectors of $x(M^n)$ in E^{n+N-1}. Then $B_\nu' \subset B_\nu$ and $\nu(B_\nu') \subset S_0^{n+N-2}$. Denote by $\bar{\nu}'$ the restriction of $\bar{\nu}$ to B_ν'. It suffices to prove that, with the exception of a set of measure zero on S_0^{n+N-2}, the points of S_0^{n+N-2} are covered by $\bar{\nu}'$ exactly twice.

Suppose the contrary be true. There is thus a set A of positive measure on S_0^{n+N-2}, whose points are covered by $\bar{\nu}'$ more than twice. To any $\mu \in A$ there are distinct points $p_1, \cdots, p_k \in M^n$, $k \geqq 3$, for which $x(p_1), \cdots, x(p_k)$ have normal vectors parallel to μ. All the unit vectors in the great circle spanned by μ and v are then normal to $x(M^n)$ at $x(p_1), \cdots, x(p_k)$. It follows that all the points of S_0^{n+N-1} belonging to great circles spanned by v and the points of A are covered by $\bar{\nu}$ more than twice. Since A has positive measure on S_0^{n+N-2}, this set has positive measure on S_0^{n+N-1}, which is a contradiction.

Therefore $x(M^n)$ belongs to E^{n+N-1} and has, as a submanifold of E^{n+N-1}, a total curvature equal to $2c_{n+N-2}$. By induction on N we see that $x(M^n)$ must belong to a linear subvariety E^{n+1} of dimension $n+1$ and has in E^{n+1} the total curvature $2c_n$.

LEMMA 2. *Let $x: M^n \rightarrow E^{n+1}$ be an immersion of a compact oriented manifold and let $\nu: M^n \rightarrow S_0^n$ be the normal map of Gauss. Let $J(p)$ be the Jacobian matrix of ν at p, and let $U_m = \{p \in M^n \mid \text{rank}\, J(p) = n - m\}$. Then, if U_m contains an open set V, its image under x is generated by m-dimensional planes. Every boundary point of U_m, which is at the same time a limit point of an m-dimensional generating plane, belongs to U_m.*

The fact that the image under x of V is generated by m-dimensional planes is a classical result; we include a proof for completeness. At any interior point p of U_m the assumption on the rank of J implies that we may choose coordinates on M^n in the neighborhood of p, say, $t_1, \cdots, t_n$, such that if ν is the unit normal vector at p, then $\partial\nu/\partial t_\alpha = 0$, and $\partial\nu/\partial t_a$ are linearly independent. Here, and for the remainder of this section, we make the following convention concerning indices:

$$1 \leqq \alpha, \beta, \gamma \leqq m, \qquad m+1 \leqq a, b, c \leqq n, \qquad 1 \leqq i, j, k \leqq n.$$

We have $\nu \cdot \partial x/\partial t_i = 0$. It follows that

$$\nu \cdot \partial^2 x/\partial t_i \partial t_\alpha = 0, \;\; \partial\nu/\partial t_\alpha \cdot \partial x/\partial t_i + \nu(\partial^2 x/\partial t_i \partial t_\alpha) = 0, \; \partial\nu/\partial t_a \cdot \partial x/\partial t_\alpha = 0.$$

Hence $\partial x/\partial t_\alpha$ are vectors orthogonal to the $n - m + 1$ linearly independent vectors ν, $\partial\nu/\partial t_a$. The surfaces $t_a = t_a{}^0 = \text{const.}$ are therefore m-dimensional planes in E^{n+1}. Since $\partial\nu/\partial t_\alpha = 0$, the tangent hyperplane remains constant along an m-dimensional generating plane.

Consider now the sub-bundle B' of B consisting of all those frames $e_1, \cdots, e_{n+1}$ such that e_α are in the m-dimensional generating planes. Then, as in Section 1, we have

$$dx = \sum_i \omega_i e_i, \quad de_i = \sum_j \omega_{ij} e_j + \omega_{i,n+1} e_{n+1}, \quad de_{n+1} = \sum_j \omega_{n+1,j} e_j,$$

where

$$\omega_{i,n+1} = \sum_j A_{ij}\omega_j, \qquad\qquad A_{ij} = A_{ji}.$$

The above assumption on the bundle of frames B' is equivalent to assuming

$$\omega_{\alpha,n+1} = -\omega_{n+1,\alpha} = 0; \tag{24}$$

i.e., that the matrix (A_{ij}) takes the form

$$\begin{pmatrix} 0 & 0 \\ 0 & A_{ab} \end{pmatrix}, \qquad \det(A_{ab}) = D \neq 0,$$

which is an $(n \times n)$-matrix whose elements are zero, except possibly those of the $(n-m)\times(n-m)$ block in the lower right-hand corner. Our proof depends on studying the behavior of D along the m-dimensional generating plane.

From (24) we have

$$0 = d\omega_{\alpha,n+1} = \sum_k \omega_{\alpha k} \wedge \omega_{k,n+1} = \sum_\beta \omega_{\alpha\beta} \wedge \omega_{\beta,n+1} + \sum_a \omega_{\alpha a} \wedge \omega_{a,n+1}.$$

Our assumption implies

$$\omega_{\beta,n+1} = 0, \qquad \omega_{a,n+1} = \sum_b A_{ab}\omega_b,$$

so that $\sum_{a,b} A_{ab}\omega_{\alpha a} \wedge \omega_b = 0$, or $\sum_a A_{ab}\omega_{\alpha a} \wedge \prod_c \omega_c = 0$. Since $\det(A_{ab}) \neq 0$, we get $\omega_{\alpha a} \wedge \prod_c \omega_c = 0$. Hence we can put

$$\omega_{\alpha a} = \sum_b h_{\alpha ab}\omega_b. \tag{25}$$

Now we have $\prod_a \omega_{a,n+1} = D \prod_c \omega_c$. Exterior differentiation of this equation gives

$$\sum_a (-1)^{a-m-1}\omega_{m+1,n+1} \wedge \cdots \wedge d\omega_{a,n+1} \wedge \cdots \wedge \omega_{n,n+1}$$
$$= dD \wedge \prod_c \omega_c + D\Big(\sum_a (-1)^{a-m-1}\omega_{m+1} \wedge \cdots \wedge d\omega_a \wedge \cdots \wedge \omega_n\Big).$$

But

$$d\omega_{a,n+1} = \sum_k \omega_{ak} \wedge \omega_{k,n+1} = \sum_b \omega_{ab} \wedge \omega_{b,n+1},$$

$$d\omega_a = \sum_k \omega_k \wedge \omega_{ka} = \sum_{\alpha,b} h_{\alpha ab}\omega_\alpha \wedge \omega_b + \sum_b \omega_b \wedge \omega_{ba}.$$

Hence $0 = dD \wedge \prod_c \omega_c + D(\sum_{a,\alpha} h_{aa\alpha}\omega_\alpha \wedge \prod_c \omega_c)$, or

$$dD + D(\sum_{a,\alpha} h_{aa\alpha}\omega_\alpha) = 0, \quad \mathrm{mod}\, \omega_c. \tag{26}$$

To complete the proof let $p \in M^n$ be a boundary point of U_m, such that $x(p)$ is a limit point of a generating m-dimensional plane L. We choose a neighborhood V of p, in which x is one-one, and we suppose that $x^{-1}(L) \subset V$. Let $\tilde{e}_1(q), \cdots, \tilde{e}_{n+1}(q)$, $q \in V$, be a local cross-section of V into B, such that, for $q \in x^{-1}(L)$, $\tilde{e}_1(q), \cdots, \tilde{e}_m(q)$ span L. Such a cross-section clearly exists. If $\tilde{\omega}_i$, $\tilde{\omega}_j$ are the restrictions of ω_i, ω_{ij} respectively to this cross-section, then $\tilde{\omega}_i$ are linearly independent and we will have

$$\tilde{\omega}_{a\alpha} = \sum_k \tilde{h}_{a\alpha k}\tilde{\omega}_k.$$

The coefficients $\tilde{h}_{\alpha ab}(q)$ are equal to the functions $h_{\alpha ab}(q)$ introduced above, for $q \in x^{-1}(L)$. Let γ be a curve in $x^{-1}(L)$ abutting at p. We have, along γ,

$$dD + D(\sum_{a,\alpha} h_{aa\alpha}\omega_\alpha) = 0.$$

It follows by integration of this differential equation that

$$D(q) = D_0 \exp(-\int \sum h_{aa\alpha}\omega_\alpha),$$

for $q \in \gamma - p_0$, where $D_0 \neq 0$ is the value of D at a fixed point of γ. Since $D(q)$ is a continuous function and since $h_{\alpha aa}$ is bounded, we conclude that $D(p) \neq 0$. This completes the proof of Lemma 2.

We now complete the proof of Theorem 3 as follows:

Let H be the space of hyperplanes of E^{n+1} (with the obvious topology). A tangent hyperplane of $x(M^n)$ is said to be of rank m, if it is tangent to $x(M^n)$at a point of $x(U_m)$ and at no point of $x(U_l)$, $l < m$. By the argument used in the proof of Theorem 2, a tangent hyperplane of rank zero does not separate the set $x(M^n)$. For otherwise there would be a neighborhood of $S_0{}^n$, whose points are covered at least three times by ν, which would be contrary to the assumption that M^n has the minimum total curvature $2c_n$.

We will show that in every neighborhood (in the space H) of a tangent hyperplane π of $x(M^n)$ there is a tangent hyperplane of rank zero. In fact, let W be such a neighborhood. Suppose $x(p)$, $p \in U_m$, be a point of contact of π. Either there is a neighborhood of p in M which belongs completely to U_m or there are points of U_l, $l < m$, in every neighborhood of p. In both cases we can find a point p_1 such that the tangent hyperplane π_1 at $x(p_1)$ belongs to W and such that p_1 has a neighborhood in M^n which belongs completely to U_l, $l \leqq m$. The image under x of this neighborhood of p_1 is generated by l-dimensional planes and the tangent hyperplane to $x(M^n)$ along the generating l-dimensional plane through $x(p_1)$ is π_1. If $x(p_2)$, $p_2 \in M^n$, is a boundary point of this l-plane, p_2 belongs to U_l by Lemma 2 and is not an interior point of U_l. Hence there exists in every neighborhood about p_2 an open set whose points are in U_k, $k < l$, and which contains a point $p_3 \in U_k$ such that the tangent hyperplane at $x(p_3)$ is in W. Continuing this process, we see that W contains a tangent hyperplane of rank zero of $x(M^n)$.

This means that every neighborhood of π in H contains a tangent hyperplane such that $x(M^n)$ lies on one side. It follows that the same is true for π itself. If ν_0 is any unit vector in E_0^{n+1}, $\nu_0 \cdot x(p)$ has a maximum and a minimum on M^n, which must be distinct, since M^n cannot be immersed in an m-dimensional hyperplane. Hence the intersection of all the half-spaces of E^{n+1} bounded by a tangent hyperplane of $x(M^n)$ and containing points of $x(M^n)$ is a closed convex set with a non-empty interior and with $x(M^n)$ on the boundary.

Since the induced homomorphism x_* of tangent spaces is one-one, x is a local homeomorphism of M into the boundary of the convex set. It follows that $x(M^n)$ is both open and closed on the boundary; thus x maps M^n onto the boundary. But the boundary of the convex set is homeomorphic to a sphere S^n and by the above M^n is a covering space of S^n under the map x. Hence, if $n \geqq 2$, x is a homeomorphism. The same is true for $n = 1$, on account of the fact that the total curvature is $2c_1$.

Conversely, let $x(M^n)$ be a convex hypersurface. It is then locally convex. By reversing the orientation of M^n if necessary, we can suppose that $G(p) \geqq 0$. Then $K^*(p) = 2G(p)$, because there are two unit normal vectors at every point. The degree of ν is

$$1/c_n \int_{M^n} G(p)\, dV = 1.$$

Hence the total curvature of $x(M^n)$ is $2c_n$.

6. A further theorem.

THEOREM 4. *Let* $x: M^n \to E^{n+1}$ *be an immersion of a closed orientable manifold and* $\nu: M^n \to S_0^n$ *the normal map. Then the following are equivalent:*

1. $\deg \nu = \pm 1$ *and the Gaussian curvature is of constant sign*;
2. *The total curvature is* $2c_n$;
3. M^n *is imbedded as a convex hypersurface.*

It suffices to prove the implications 1) $\Rightarrow$ 2) $\Rightarrow$ 3) $\Rightarrow$ 1). Since 2) $\Rightarrow$ 3) $\Rightarrow$ 1) are contained in Theorem 3, we only have to prove that 1) implies 2).

For this purpose it is sufficient to show that no set V of positive measure on S_0^n is covered more than once by M^n under ν. Suppose the contrary. By reversing the orientation of M^n if necessary, we can suppose that $\deg \nu = +1$ and that the Gaussian curvature is non-negative. By Sard's theorem, there exists a point $y \in V$ such that for any point in $\nu^{-1}(y)$ the curvature is strictly positive. There can only be a finite number of points in $\nu^{-1}(y)$. For otherwise $\nu^{-1}(y)$ will have a limit point p at which ν is not locally one-one, while, on the other hand, the Jacobian of ν at $p \in \nu^{-1}(y)$, being a non-zero multiple of the Gaussian curvature at p, is different from zero. By our assumption on V the number of points in $\nu^{-1}(y)$ is $\geqq 2$. At each point of $\nu^{-1}(y)$ the Jacobian of ν is strictly positive. It follows that $\deg \nu \geqq 2$, which contradicts our assumption. Hence the theorem is proved.

Remark. We would like to conjecture that for $n \geqq 2$ the condition $\deg \nu = 1$ in 1) can be omitted. In other words, it seems likely that a closed orientable hypersurface (of dimension $\geqq 2$) of non-negative Gauss-Kronecker curvature is convex. If the curvature is strictly positive, this follows from Hadamard's principle. On the other hand, it is well-known that this condition is essential for $n = 1$; there are non-convex immersed curves in the plane with non-negative curvature.

UNIVERSITY OF CHICAGO.

REFERENCES.

[1] S. Chern, "La géométrie des sous-variétés d'un espace euclidien à plusieurs dimensions," *L'Enseigement Mathématique*, vol. 40 (1955), pp. 26-46.

[2] I. Fary, "Sur la courbure totale d'une courbe gauche faisant un noeud," *Bull. Soc. Math. de France*, vol. 77 (1949), pp. 128-138.

[3] J. W. Milnor, "On the total curvature of knots," *Annals of Mathematics*, vol. 52 (1950), pp. 248-257.

[4] ———, "On manifolds homeomorphic to the seven-sphere," *ibid.*, vol. 64 (1956), pp. 399-405.

[5] G. Reeb, "Sur certaines propriétés topologiques des variétés feuilletées, *Actual. Sci. et Indus.*, vol. 1183 (1952), pp. 91-154, Paris.

[6] G. de Rham, *Variétés différentiables* (1955), Paris.

SUR LES REVÊTEMENTS NON RAMIFIÉS DES VARIÉTÉS ALGÉBRIQUES.*

par Serge Lang et Jean-Pierre Serre.

Introduction. Soit V une variété algébrique normale définie sur le corps $\boldsymbol{C}$ des nombres complexes. Munissons V de la topologie "usuelle," déduite de celle de $\boldsymbol{C}$. Tout revêtement algébrique non ramifié de V peut être considéré comme un revêtement topologique, et correspond donc à un sous-groupe d'indice fini du groupe fondamental $\pi_1(V)$ de V. Des propriétés connues du groupe fondamental résulte alors immédiatement:

a) Si V et W sont deux variétés, tout revêtement de $V \times W$ est quotient d'un revêtement de la forme $V' \times W'$, où V' et W' sont des revêtements de V et de W.

(C'est une conséquence de l'égalité $\pi_1(V \times W) = \pi_1(V) \times \pi_1(W)$).

b) Le nombre des revêtements de V de degré donné est fini.

(C'est une conséquence du fait que $\pi_1(V)$ peut être engendré par un nombre fini d'éléments).

Dans ce qui suit, nous nous proposons de donner des démonstrations *algébriques* de a) et de b), valables en toute caractéristique (cf. th. 1 et th. 4) ; nous devons toutefois faire l'hypothèse supplémentaire que V est une variété *complète*. Des contre-exemples simples (dus essentiellement à la présence de "ramification supérieure") montrent d'ailleurs que a) et b) ne sont pas vrais sans restriction en caractéristique $p > 0$.

Comme application de a), nous démontrons que tout revêtement non ramifié d'une variété abélienne est une isogénie (th. 2), généralisant ainsi un résultat bien connu pour les courbes elliptiques.

1. Conventions et notations. Nous adopterons la définition des *revêtements* donnée dans [4] § 1, à cela près que nous ne nous occuperons que de revêtements *géométriques*. Par définition, un revêtement est donc une application rationnelle partout définie

$$f\colon U \rightarrow V,$$

---

[1] Received December 21, 1956.

vérifiant les conditions suivantes:

α) U et V sont des variétés *normales* (absolument irréductibles) de même dimension.

β) Pour tout $v \in V$, l'ensemble $f^{-1}(v)$ est *fini.*

γ) La variété U est *complète* au-dessus de tout point de V.

δ) Si K et L désignent les corps des fonctions rationnelles sur V et sur U, l'extension L/K est *séparable.*

Si U, V et f sont définis sur un corps k, on dira plus brièvement que le revêtement est défini sur k.

Les propriétés ci-dessus entraînent que U est la normalisée de V dans l'extension L/K (pour tout ce qui concerne l'operation de normalisation, voir par exemple [6], Chap. II, § 5) ; inversement, si l'on se donne une variété normale V ayant K pour corps de fonctions, et si l'on se donne une extension finie séparable L de K, la normalisée U de V dans L/K est un revêtement de V. Ainsi, V étant donnée, il y a correspondance bijective entre revêtements de V et extensions finies séparables de K. Le *degré* de l'extension L/K sera appelé le degré du revêtement $f\colon U \rightarrow V$, et sera noté $[U\colon V]$. De même, un revêtement sera dit *galoisien,* de groupe de Galois G, si l'extension L/K correspondante est galoisienne et de groupe de Galois G; on a alors $V = U/G$, avec les notations de [7], no. 13.

Soit $f\colon U \rightarrow V$ un revêtement de degré n, défini sur un corps algébriquement clos k. Si v est un point de V, l'ensemble $f^{-1}(v)$ a au plus n éléments; s'il en a exactement n, on dira que U est *non ramifié en v.* L'ensemble des points de ramification est un sous-ensemble k-fermé de V; s'il est vide, on dira que U est *non ramifié.* En fait, pour qu'une application rationnelle partout définie $f\colon U \rightarrow V$ soit un revêtement non ramifié, il suffit, d'après Krull ([2], voir aussi [4], p. 292), que V soit normale, que les conditions β) et γ) soient remplies, et que pour tout point $v \in L$ l'ensemble $f^{-1}(v)$ ait exactement n points (n désignant comme précédemment le degré de l'extension L/K) ; la variété U est alors automatiquement normale, et l'extension L/K séparable.

Revenons au cas d'un revêtement quelconque $f\colon U \rightarrow V$, et soit V' une sous-variété de V. Soit $f^{-1}(V')$ l'image réciproque de V' dans U, et soient U_i' les composantes irréductibles de $f^{-1}(V')$. En appliquant les théorèmes du type Cohen-Seidenberg, on voit tout de suite que les U_i' ont même dimension que V'; de plus, si l'on note $[U_i'\colon V']$ le degré de la projection $U_i' \rightarrow V'$, on a:

$$\Sigma[U_i'\colon V'] \leqq [U\colon V], \text{ cf. [2] ainsi que [4], } \textit{loc. cit.}.$$

Lorsque tous les degrés $[U_i' \colon V']$ sont égaux à 1, on dira que le revêtement U *se décompose complètement* sur V'.

En général, les U_i' ne sont pas des variétés normales, et les extensions de corps correspondant aux projections $U_i' \to V'$ ne sont pas séparables. On a toutefois:

LEMME 1. *Supposons que le revêtement* $f\colon U \to V$ *soit non ramifié, et soit* V' *une sous-variété normale de* V. *Alors les composantes* U_i' *de* $f^{-1}(V')$ *sont des variétés normales et disjointes. Chacune d'elles est un revêtement non ramifié de* V', *et l'on a l'égalité:*

$$\Sigma[U_i' \colon V'] = [U \colon V].$$

Posons $n = [U \colon V]$ et $n_i = [U_i' \colon V']$; d'après ce qui a été dit plus haut, on a en tout cas $\Sigma n_i \leqq n$. D'autre part, soit $v \in V'$, et soit m_i le norbre des points de U_i' se projetant en v; du fait que V' est normale, on a $m_i \leqq n_i$. Mais d'autre part, puisque $f\colon U \to V$ est non ramifié, il a exactement n points de U qui se projettent en v. On a donc $\Sigma m_i \geqq n$, d'où $m_i = n_i$ et $\Sigma n_i = n$. D'après le résultat de Krull déjà cité, l'égalité $m_i = n_i$ entraîne que U_i' est un revêtement non ramifié de V', et en particulier que U_i' est une variété normale; enfin, si U_i' et U_j' avait en commun un point u, de projection v, l'ensemble des points de U se projetant en v aurait au plus $\Sigma m_i - 1 = n - 1$ éléments, ce qui est impossible; les variétés U_i' sont donc bien disjointes, ce qui achève la démonstration.

(Notons que, si $f\colon V \to V$ est galoisien, il en est de même de chacun des revêtements $U_i' \to V'$; leurs groupes de Galois sont des sous-groupes de celui de U—les classiques "groupes de décomposition").

Plus généralement, soit $\alpha\colon V' \to V$ une application partout définie d'une variété V' dans V; supposons encore que V' soit normale. Alors $V' \times U$ forme de façon naturelle un revêtement de $V' \times V$; si l'on plonge V' dans $V' \times V$ au moyen du graphe de α, on peut encore définir $f^{-1}(V') \subset V' \times U$, et l'on se retrouve dans la situation envisagée ci-dessus; dans la suite, nous noterons $\alpha^*(U)$ l'ensemble algébrique $f^{-1}(V')$; par définition, c'est l'ensemble des couples $(v', u) \in V' \times U$ tels que $\alpha(v') = f(u)$. Lorsque U est non ramifié, le lemme 1 montre que les composantes irréductibles de $\alpha^*(U)$ sont des revêtements non ramifiés de V' (les "pull-back" de [4], § 4).

2. Revêtements d'un produit de variétés. Soient V et W deux variétés normales. Dans ce no., nous aurons à considérer des revêtements du produit $V \times W$. Si $f\colon U \to V \times W$ est un tel revêtement, et si w est un point de W, nous noterons U_w l'image réciproque de $V \times \{w\}$ dans U; si l'on note α_w l'injection de V dans $V \times W$ définie par la formule $\alpha_w(v) = (v, w)$, l'ensemble algébrique U_w n'est autre que $\alpha_w^*(U)$. Lorsque U est non ramifié, les composantes irréductibles de U_w sont des revêtements non ramifiés de V, d'après le lemme 1.

LEMME 2. *Soit k un corps de définition d'un revêtement $f\colon U \rightarrow V \times W$, et soit w un point générique de W sur k. Supposons que U soit complètement décomposé sur $V \times \{w\}$. Alors U est isomorphe à un revêtement $V \times W'$, où W' est un revêtement de W.*

Soit v un point générique de V, indépendant de w, et soit $u \in U$ tel que $f(u) = (v, w)$; le point u est alors un point générique de U sur k. On voit tout de suite que le lieu de u sur le corps $k(w)$ n'est autre que U_w, qui est donc irréductible sur $k(w)$. Soit L la fermeture algébrique de $k(w)$ dans $k(u)$; par hypothèse, $k(u)/k(v, w)$ est séparable, et il en est évidemment de même de $k(v, w)/k(w)$; donc $k(u)/k(w)$ est séparable, et l'extension $k(u)/L$ est régulière. Il s'ensuit que le lieu de u sur L est l'une des composantes irréductibles de U_w; puisque on a supposé U complètement décomposé sur $V \times \{w\}$, on a donc $k(u) = L(v)$. Si l'on désigne alors par W' la normalisée de W dans l'extension $L/k(w)$, la variété $V \times W'$ est la normalisée de $V \times W$ dans $k(u)/k(v, w)$, donc est isomorphe à U, cqfd.

Remarque. Le lemme 2 ne s'étend pas aux "revêtements inséparables" (c'est-à-dire ceux où l'on supprime l'hypothèse δ) du no. 1). Pour le voir, il suffit de poser $k(w) = k(x, y)$ et $k(u) = k(v, x, y, \theta)$, avec $\theta^p = x + v^p y$, k désignant un corps algébriquement clos de caractéristique p.

LEMME 3. *Soit $f\colon U \rightarrow V \times W$ un revêtement non ramifié, V étant un variété complète. Supposons qu'il existe $a \in W$ tel que U se décompose complètement sur $V \times \{a\}$. Alors U est isomorphe à un revêtement $V \times W'$, où W' est un revêtement non ramifié de W.*

Supposons d'abord que V soit une variété *projective*. Soit k un corps de définition du revêtement, et soit w un point générique de W par rapport à k. D'après le théorème de dégénérescence de Zariski ([8]), le nombre de composantes connexes de U_w est au moins égal à celui de sa spécialisation U_a; mais, d'après le lemme 1, ce dernier nombre est égal à celui des composantes irréductibles de U_a, lequel est égal à $[U : V]$ par hypothèse. Il s'ensuit que le nombre de composantes connexes de U_w est aussi égal à $[U : V]$, ce qui signifie que U se décompose complètement sur $V \times \{w\}$;

d'après le lemme 2, il s'ensuit que $U = V \times W'$, et on voit immédiatement que W' est non ramifié.

L'hypothèse que V est projective n'a été appliquée que pour pouvoir utiliser le théorème de dégénérescence de Zariski. Le cas général se ramène au cas projectif: d'après un résultat de Chow (cf. [1]), il existe une variété projective normale V_1 et une application birationnelle partout définie

$$\phi\colon V_1 \to V.$$

L'application ϕ définit une application $\psi\colon V_1 \times W \to V \times W$; posons $U_1 = \psi^*(U)$; en appliquant la première partie de la démonstration à U_1, on voit que $U_1 = V_1 \times W'$. Le corps $k(U_1)$ des fonction rationnelles sur U_1 est donc un composé $k(V_1) \cdot k(W') = k(V) \cdot k(W')$; il s'ensuit que $k(U) = k(V) \cdot k(W')$, d'où $U = V \times W'$, cqfd.

Remarque. Le lemme 3 est inexact lorsque l'on ne suppose plus que V est complète: on le voit en prenant pour V et W des droites affines de points génériques v et w, et en définissant U par l'équation $u^p - u = vw$ (si l'on fait $v = 0$ ou $w = 0$, l'équation se décompose, ce qui serait incompatible avec le lemme 3).

THÉORÈME 1. *Soit $f\colon U \to V \times W$ un revêtement non ramifié, V étant une variété complète. Il existe alors deux revêtements non ramifiés V' de V et W' de W tels que U soit un quotient du revêtement produit $V' \times W'$.*

Nous pouvons évidemment supposer que le revêtement U est galoisien; soit G son groupe de Galois. Choisissons alors un point $a \in W$, et soit $U_a = f^{-1}(V \times \{a\})$; d'après le lemme 1, les composantes irréductibles de U_a sont des revêtements non ramifiés de V; comme on a supposé U galoisien, il en sera de même pour ces composantes (leurs groupes de Galois étant des sous-groupes de G, les "groupes de décomposition"). Choisissons l'une de ces composantes, soit V', et soit $G' \subset G$ son groupe de Galois. La projection $V' \to V$ définit une projection

$$h\colon V' \times W \to V \times W,$$

qui fait de $V' \times W$ un revêtement de $V \times W$ de groupe de Galois G'. Posons $U = h^*(U)$, sous-ensemble algébrique de $V' \times W \times U$; comme précédemment pour U_a, les composantes irréductibles de U_1 sont des revêtements non ramifiés de $V' \times W$, galoisiens et de groupes de Galois des sous-groupes de G. Soit $b \in V'$ et soit U' la composante de U_1 qui contient le point $(b, a, b) \in U_1$; comme U' est un revêtement non ramifié de $V' \times W$, c'est aussi un revêtement non ramifié de $V \times W$; de plus, puisque la projection de U' sur $V \times W$ se factorise en $U' \to U \to V \times W$, le revêtement U est un quotient de U', et il nous suffira donc de prouver que U' est de la forme $V' \times W'$. Mais U' se décompose complètement sur $V' \times \{a\}$: en effet, U_1 contient la sous-variété de $V' \times W \times U$ formée des points (v', a, v') où v' parcourt V'; comme cette sous-variété a le point (b, a, b) en commun avec U', elle est contenue dans U', et constitue une composante de U_a' se projetant sur $V' \times \{a\}$ avec degré 1; du fait que U' est galoisien, ceci suffit à assurer que U' se décompose complètement sur $V' \times \{a\}$. En appliquant alors le lemme 3, on en déduit bien que U' est isomorphe à un revêtement de la forme $V' \times W'$, ce qui achève la démonstration.

COROLLAIRE 1. *Soit G un groupe abélien fini. Les notations étant celles de* [7], no. 14, *on a* $\pi^1(V \times W, G) = \pi^1(V, G) \times \pi^1(W, G)$.

C'est immédiat.

COROLLAIRE 2. *Les hypothèses étant celles du théorème* 1, *soient a et b deux points de W. Il existe alors un isomorphisme de l'ensemble algébrique U_a sur l'ensemble algébrique U_b compatible avec les projections $U_a \to V$ et $U_b \to V$.*

(On a un énoncé analogue en permutant les rôles de V et de W).

En effet, d'après le théorème 1, le revêtement U est quotient d'un revêtement g: $V' \times W' \to V \times W$; on peut supposer V' et W' galoisiens de groupes de Galois G_1 et G_2 respectivement; alors U est isomorphe à $(V' \times W')/H$, où H est un sous-groupe de $G_1 \times G_2$. Posons:

$$U_a' = g^{-1}(V \times \{a\}) \quad \text{et} \quad U_b' = g^{-1}(V \times \{b\}).$$

Il est clair que U_a' et U_b' sont tous deux isomorphes à $V' \times G_2$, ces isomorphismes commutant avec les opérations de $G_1 \times G_2$; comme U_a est isomorphe à U_a'/H, il est isomorphe à $(V' \times G_2)/H$, et de même pour U_b, ce que démontre le corollaire.

Lorsque U est galoisien, de groupe de Galois G, on a $G = (G_1 \times G_2)/H$; de plus, on peut supposer (quitte à changer V' et W') que $G_1 \cap H = \{e\}$ et $G_2 \cap H = \{e\}$. Les groupes G_1 et G_2 s'identifient ainsi à des sous-groupes de G, invariants, commutant entre eux, et engendrant G. De plus, le raisonnement fait ci-dessus montre que, pour tout $a \in W$, l'ensemble algébrique U_a se décompose en composantes irréductibles qui sont isomorphes à V', le groupe G_1 s'identifiant au groupe de décomposition correspondant; on a un résultat analogue pour U_v si $v \in V$. En définitive, on a obtenu:

COROLLAIRE 3. *Outre les hypothèses du théorème* 1, *supposons que U soit galoisien de groupe de Galois G. Soit $(v,w) \in V \times W$, et soit V' (resp. W') une composante de U_w (resp. U_v); soit G_1 (resp. G_2) son groupe de Galois. Les groupes G_1 et G_2 sont alors des sous-groupes invariants de G, qui commutent entre eux et engendrent G; si H désigne le noyau de l'homomorphisme $G_1 \times G_2 \rightarrow G$, le revêtement U est isomorphe à $(V' \times W')/H$.*

3. Revêtements non ramifiés des variétés abéliennes. Nous nous proposons de démontrer le résultat suivant:

THÉORÈME 2. *Toute revêtement non ramifié d'une variété abélienne est une isogénie* (*séparable*).

(Cela montre en particulier qu'un tel revêtement est *abélien*).

Soit donc V une variété abélienne, et soit $f\colon U \rightarrow V$ un revêtement non ramifié de V. On peut évidemment supposer que U est galoisien; soit G son groupe de Galois. Il nous faut montrer que l'on peut définir sur U une structure de variété abélienne (auquel cas f sera automatiquement une isogénie).

Soit $g\colon V \times V \rightarrow V$ l'application qui définit la loi de composition de V, i.e. $g(v,v') = v + v'$. Soit $U' = g^*(U)$, sous-ensemble algébrique de $V \times V \times U$ formé des triples (v,v',u) tels que $f(u) = v + v'$. Le groupe G permute les composantes irréductibles de U'; mais si l'on pose

$$U_1' = U' \cap (\{0\} \times V \times U),$$

l'ensemble U_1' s'identifie à U, donc est irréductible; *a fortiori*, il en est de même de U'. Nous noterons $f'\colon U' \rightarrow V \times V$ la projection de U' sur les deux premiers facteurs du produit $V \times V \times U$. On a évidemment $U_1' = f'^{-1}(\{0\} \times V)$, et l'on vient de voir que U_1' s'indentifie à U; de même $U_2' = f'^{-1}(V \times \{0\})$ s'identifie à U. Appliquant alors le corollaire 3 au théorème 1, on voit que. avec les notations de ce corollaire, on a $G_1 = G_2 = G$, ce qui montre d'abord que G est *abélien*, puis que U' s'identifie à $(U \times U)/H$, où H désigne le sous-groupe de $G \times G$ formé par les éléments (g, g^{-1}), $g \in G$. Comme on a une application canonique $h\colon U' \rightarrow U$, on en déduit par composition une application $g'\colon U \times U \rightarrow U' \rightarrow U$ qui "relève" l'application $g\colon V \times V \rightarrow V$. Si l'on a choisi dans U un point e tel que $f(e) = 0$, on peut en outre s'arranger pour que $g'(e,e) = e$. Il ne nous reste plus qu'à démontrer que l'application g' vérifie les axiomes d'une loi de groupe, ce que ne présente pas de difficultés:

a) Le point $e \in U$ est élément neutre pour la loi de composition g'. En effet, soit $\sigma\colon U \to U$ l'application définie par la formule:

$$\sigma(u) = g'(e, u).$$

On a $f \circ \sigma = f$, ce qui montre que σ est un automorphisme du revêtement U, i.e. un élément du groupe de Galois G. Mais on a $\sigma(e) = e$, et comme G opère sans points fixes, cela montre que σ est l'identité; un raisonnement analogue montre que $g'(u, e) = u$ pour tout $u \in U$.

b) La loi de composition g' est associative.

Soient k_1 et k_2 les applications de $U \times U \times U$ dans U définies par les formules:

$$k_1(v, v', v'') = g'(v, g'(v', v'')) \quad \text{et} \quad k_2(v, v', v'') = g'(g'(v, v'), v'').$$

Du fait que g' relève g, les projections de $k_1(v, v', v'')$ et de $k_2(v, v', v'')$ dans U sont les mêmes. On a donc $k_2(v, v', v'') = \sigma \cdot k_1(v, v', v'')$, avec $\sigma \in G$. Appliquons ceci à trois points génériques indépendants v, v', v''; en spécialisant v, v' et v'' en e, on voit que $\sigma = 1$, d'où $k_1 = k_2$ et g' est bien une loi de composition associative.

c) Il existe un inverse $u \to u^{-1}$ qui est un automorphisme de U.

Désignons par f'' l'application $f \times f\colon U \times U \to V \times V$; soit d'autre part $\phi\colon V \times V \to V \times V$ l'application définie par $(v, v') \to (v, v + v')$, et soit de même $\psi\colon U \times U \to U \times U$ l'application définie par

$$\psi(u, u') = (u, g'(u, u')).$$

On a évidemment la relation de commutation $f'' \circ \psi = \phi \circ f''$. En prenant les degrés des deux membres, et en tenant compte du fait que ϕ est birationnelle, on voit qu'il en est de même de ψ. De plus, ψ est partout définie puisque ϕ l'est. L'existence d'un inverse, et le fait que $u \to u^{-1}$ est un automorphisme résultent aussitôt de là, ce qui achève la démonstration.

Remarques.

1) La démonstration précédente est calquée sur la démonstration classique prouvant que tout revêtement d'un groupe topologique est un groupe topologique (démonstration qui repose elle-même sur la formule $\pi_1(X \times Y) = \pi_1(X) \times \pi_1(Y)$).

2) Le théorème 2 *ne s'étend pas* aux groupes algébriques non complets. On trouvera des contre-exemples dans [3], relatifs au cas où V est un groupe

non commutatif, défini sur un corps fini. En fait, on peut même construire des contre-exemples où V est le groupe additif G_a: si U' est une courbe elliptique d'invariant de Hasse nul, une différentielle de première espèce de U' peut s'écrire $\omega = df$, où f est une fonction rationnelle; soit U l'ouvert de U' obtenu en retirant l'ensemble des pôles de f; il est clair que $f\colon U \to G_a$ est un revêtement non ramifié qui n'est pas une isogénie.

4. Finitude du nombre des classes de revêtements non ramifiés d'une variété complète. Nous démontrerons d'abord le résultat suivant:

THÉORÈME 3. *Soit V une variété normale, complète, définie sur un corps algébriquement clos k. Alors tout revêtement non ramifié de V est isomorphe à un revêtement défini sur k.*

(Autrement dit, il n'y a pas de "systèmes algébriques" de revêtements non ramifiés).

Soit $f_1\colon U_1 \to V$ un revêtement non ramifié de V, défini sur une extension L/k que l'on peut supposer de type fini. Soient v un point générique de V sur L et u un point de U_1 tel que $f_1(u) = v$. Soit d'autre part W' une variété normale, définie sur k, telle que, si w est un point générique de W' sur k, on ait $L = k(w)$. On a $L(v) = k(v, w)$, corps des fonctions rationnelles sur $V \times W'$, et le corps $L(u)$ est une extension finie de $k(v, w)$. Soit U' la normalisée de $V \times W'$ dans l'extension $L(u)/k(v, w)$, et soit f la projection canonique de U' sur $V \times W'$. It est clair que $U_w' = f^{-1}(V \times \{w\})$ est une variété $k(w)$-normale, et en correspondance birationnelle, sur $k(w)$, avec le revêtement donné U_1; comme U_1 est normale, ceci montre que U_w' et U_1 sont isomorphes. Soit $Z \subset V \times W'$ l'ensemble des points au-dessus desquels le revêtement U' est ramifié; c'est un ensemble algébrique k-fermé, qui ne rencontre pas $V \times \{w\}$ puisque par hypothèse $U_1 = U_w'$ est non ramifié. Il est donc contenu dans un produit $V \times Z'$, où Z' est un sous-ensemble algébrique k-fermé de W'; posons $W = W' - Z'$, et soit U l'image réciproque de $V \times W$ dans U'. Le revêtement U est non ramifié, et l'on a $U_w = U_w' = U_1$; choisissons alors dans W un point a, rationnel sur k. D'après le corollaire 2 au théorème 1 les ensembles algébriques U_w et U_a sont isomorphes. Il s'ensuit que U_a est irréductible, et que c'est un revêtement de V isomorphe à U_1, cfqd.

THÉORÈME 4. *Une variété normale et complète ne possède qu'un nombre fini de revêtements non ramifiés de degré donné.*

Soit V une telle variété. D'après Chow [1], V est image d'une variété projective V_1, que l'on peut supposer normale, et qui est birationnellement équivalente à V. Tout revêtement non ramifié de V en définit un de V_1, et l'on est ainsi ramené à démontrer le théorème pour V_1. Autrement dit, nous pouvons supposer que V est une variété *projective.* Soit k un corps de définition de V, et soit C_u une *courbe générique* de V (sur k), au sens défini dans [5], § 3; on sait (*loc. cit.*) que si U est un revêtement de V, défini sur k, la restriction de U à C_u est un revêtement irréductible de C_u. Il s'ensuit, par un raisonnement standard, que deux revêtements non isomorphes de V, tous deux définis sur k, ont des restrictions à C_u qui sont également non isomorphes. En prenant pour k un "domaine universel," on voit donc qu'il suffira de démontrer le théorème 4 pour C_u.

Nous supposerons donc, à partir de maintenant, que V est une *courbe* C, non singulière, complète, de genre g. Nous la supposerons plongée dans un espace projectif S_1, et nous désignerons son degré projectif par d. Si $f\colon U \to C$ est un revêtement non ramifié de C de degré n, le genre g_U de la courbe U est donné par la formule classique:

$$g_U - 1 = n(g-1),$$

et ne dépend donc pas de U. D'après le théorème de Riemann-Roch, on peut plonger birégulièrement U dans un espace projectif S_2 de dimension g_U (donc fixe), le degré projectif de ce plongement étant $d_2 = 2g_U + 1$. Soit $\Gamma \subset S_1 \times S_2$ le graphe de f. Si H_1 et H_2 sont des hyperplans de S_1 et S_2, posons:

$$H = S_1 \times H_2 + H_1 \times S_2;$$

un calcul immédiat montre que $\deg(\Gamma \cdot H) = d_2 + nd$, donc que ce degré ne dépend pas de U. Cela signifie que, si l'on plonge $S_1 \times S_2$ dans un espace projectif S_3 à la manière habituelle (i.e. de telle sorte que H devienne une section hyperplane dans ce nouveau plongement), le degré de Γ dans S_3 sera $d_2 + nd$, donc sera fixe.

Or, d'après la théorie des coordonnées de Chow, il n'existe qu'un nombre *fini* de familles algébriques irréductibles de cycles de $C \times S_2$ ayant un degré donné (dans S_3). Il nous suffit donc de prouver que, si deux revêtements U_1 et U_2 ont des graphes Γ_1 et Γ_2 qui appartiennent à la même famille algébrique F, ces deux revêtements sont isomorphes.

Pour cela, soit Γ un élément générique de la famille F; nous allons d'abord montrer que $\Gamma \to C$ est un revêtement non ramifié de degré n. Tout d'abord, puisque Γ admet pour spécialisation Γ_1, c'est une variété; comme la projection sur C est compatible avec les spécialisations, la relation

$\mathrm{pr}_1(\Gamma_1) = nC$ entraîne $\mathrm{pr}_1(\Gamma) = nC$, donc l'application $\Gamma \rightarrow C$ est de degré n. De plus, si Q est un point de C, on peut prolonger la spécialisation $\Gamma \rightarrow \Gamma_1$ en une spécialisation $Q \rightarrow Q_1$, et $Q \times S_2$ se spécialise en $Q_1 \times S_2$. Comme le cycle $\Gamma_1 \cdot (Q_1 \times S_2)$ est défini, et se compose de n points distincts, il en est de même du cycle $\Gamma \cdot Q \times S_2)$. D'après ce qu'on a vu au no. 1, il s'ensuit bien que Γ est un revêtement non ramifié de degré n de la courbe C.

Nous allons maintenant montrer que les revêtements Γ_1 et Γ sont isomorphes; comme le même argument montrera que Γ_2 et Γ sont isomorphes, il en résultera bien que Γ_1 et Γ_2 sont isomorphes, ce qui achèvera la démonstration, en vertu de ce qui a été dit plus haut.

D'après le théorème 3, le revêtement Γ est isomorphe à un revêtement Γ' défini sur le corps de base; on peut supposer Γ' plongé dans $C \times S_2$ comme ci-dessus. Désignons par T le graphe de l'isomorphisme $\Gamma \rightarrow \Gamma'$; c'est une sous-variété de $\Gamma \times \Gamma'$, lui-même contenu dans $C \times S_2 \times C \times S_2$. On a évidemment $\mathrm{pr}_{13}(T) = n\Delta$, où Δ est la diagonale de $C \times C$. Etendons maintenant la spécialisation $\Gamma \rightarrow \Gamma_1$ en une spécialisation $T \rightarrow T_1$; la variété Γ' reste fixe durant cette spécialisation, puisqu'elle est définie sur le corps de base. On a $\mathrm{pr}_{12}(T_1) = \Gamma_1$, $\mathrm{pr}_{34}(T_1) = \Gamma'$ et $\mathrm{pr}_{13}(T_1) = n\Delta$; les deux premières formules montrent que, ou bien T_1 est le graphe d'une correspondance birationnelle entre Γ_1 et Γ', ou bien T_1 est "dégénérée," i.e. égale à $\Gamma_1 \times \{\gamma'\} + \{\gamma_1\} \times \Gamma'$; la troisième formule exclut cette seconde possibilité. On a donc obtenu une correspondance birationnelle entre les revêtements Γ_1 et Γ', commutant avec les projections sur C. Il s'ensuit que Γ_1 et Γ' sont isomorphes, donc aussi Γ_1 et Γ, cqfd.

Remarques.

1) La démonstration du théorème 4 que nous venons de donner utilise de façon essentielle les résultats du no. 2. Inversement, si l'on pouvait démontrer directement le théorème 4 (dans le cas d'une courbe), on retrouverait facilement ces résultats comme corollaires.

2) Soit C une courbe, et soient $P_1, \cdots, P_r$ des points de C en nombre fini. Il est vraisemblable qu'il n'existe qu'un nombre fini de revêtements de C d'un degré n donné, ramifiés seulement aux points P_i, et n'y admettant pas de ramification supérieure (revêtements "tamely ramified"). Une démonstration de ce fait permettrait d'étendre notablement nos résultats.

3) Dans le cas des revêtements abéliens, le théorème 4 peut aussi se démontrer en utilisant le théorème de Néron-Severi (pour les revêtements d'ordre premier à la caractéristique), et la finitude du premier groupe de

cohomologie (pour les revêtements d'ordre une puissance de la caractéristique). Cf. [7], nos. 15 et 16.

COLUMBIA UNIVERSITY
INSTITUTE FOR ADVANCED STUDY.

BIBLIOGRAPHIE.

[1] W-L. Chow, "On the projective embedding of homogeneous varieties," *Symposium in honor of S. Lefschetz*, Princeton, 1957.

[2] W. Krull, "Der allgemeine Diskriminantensatz. Unverzweigte Ringerweiterungen," *Mathematische Zeitschrift*, vol. 45 (1939), pp. 1-19.

[3] S. Lang, "Algebraic groups over finite fields," *American Journal of Mathematics*, vol. 78 (1956), pp. 555-563.

[4] ———, "Unramified class field theory over function fields in several variables," *Annals of Mathematics*, vol. 64 (1956), pp. 285-325.

[5] ———, "Sur les séries L d'une variété algébrique," *Bulletin de la Société Mathématique de France*, vol. 84 (1956), pp. 385-407.

[6] M. Nagata, "A general theory of algebraic geometry over Dedekind domains. I. The notion of models," *American Journal of Mathematics*, vol. 78 (1956), pp. 78-116.

[7] J-P. Serre, "Sur la topologie des variétés algébriques en caractéristique p," *Symposium de topologie algébrique*, Mexico, 1956.

[8] O. Zariski, "Theory and applications of holomorphic functions on algebraic varieties over arbitrary ground fields," *Memoirs of the American Mathematical Society*, No. 5, 1951.

LIE GROUPS AND LIE HYPERALGEBRAS OVER A FIELD OF CHARACTERISTIC $p > 0$ (VI).*

By JEAN DIEUDONNÉ.

1. Introduction. In the preceding papers of this series ([8] to [12])[1] our main task had been the study of *abelian* formal Lie groups, and the general theory had not been developed beyond the most elementary theorems. On the contrary, this paper is chiefly devoted to *noncommutative* formal Lie groups. There seems to be little hope at present of using the hyperalgebras, in that part of the theory, to the same effect as they were used in the study of abelian groups [11]. Here the hyperalgebra recedes in the background and becomes a mere technical tool, and the method of attack is based on an entirely different idea, which consists in considering the homomorphisms of a formal Lie group G into *linear groups.* When G has *no center,* there exist such homomorphisms which are injective; when such homomorphisms exist (in which case G is said to be *representable*), it is possible to define an "algebraic hull" of the image of G by such a homomorphism, following the pattern of the corresponding techniques used by C. Chevalley for Lie algebras [6] and by A. Borel for arbitrary (non formal) subgroups of linear groups [2]. I must record here my indebtedness to these two fundamental papers: not only do they suggest, by analogy, the results to be expected for

---

* Received November 28, 1956.

[1] I take this opportunity to correct a few misprints and minor errors in these papers: in [9], p. 237, formula (45), the summation should extend over the range $0 < \mu < \lambda$. In [10], p. 64, in lines 1-2 from top, the condition "et n'ont aucune composante d'indice $< i$ qui soit non nulle" should be omitted, as well as the statement "toutes les composantes d'indice $< i$ sont nulles" in lines 12-13 from top. On the same page, the index (or exponent) i in G_i, $\bar{G}_i$, $\mathfrak{m}_i$, $\bar{\mathfrak{m}}_i$, $u^{(i)}$, $\bar{u}^{(i)}$ should be replaced by $i+1$. On p. 69 of the same paper, equation (39) should read $\Delta(\mathrm{Hex}(x_0, x_1, \cdots)) = c \cdot \mathrm{Hex}(x_0, x_1, \cdots)$ where c is a constant, and in line 10 from bottom, y should be replaced by x. In [12,] p. 208, line 9 from top, read $<$ instead of $\leqq$; p. 210, line 9 from top, read $\xi^{p^{-1}}$; p. 211, lines 3 and 6 from bottom, replace r by $r+1$; p. 219, line 12 from bottom, there should be a bar over the second $\mathfrak{r}_{m+1}$; p. 221, line 4 from top, there should be a bar over $\mathfrak{q}_{m+1,r}$; p. 222, line 14 from bottom, replace p^r by p^{r+1}; p. 238, formula (65), read $E(Y_1^{(q,2)})$ instead of $(Y_1^{(q,2)})$. In [13], p. 252, formula (3), the summation is over the index α; p. 254, line 18 from top, X_{hi} should be replaced by $\bar{X}_{hi}$. P. 255, line 3 from bottom, p. 256, line 10 from top, p. 257, line 18 from bottom, replace the exponent β_{k-1} by $\beta_k - 1$.

formal Lie groups, and sometimes the methods of proof by which they can be obtained, but it turns out that a surprisingly large number of the theorems of A. Borel for *algebraic* groups can be used to prove their counterparts for *formal* Lie groups (even when there does not seem to be any possibility of extending their *method* of proof): we mention in particular many of Borel's results on solvable maximal subgroups, maximal tori and Cartan subgroups. This is mainly due to a fundamental result (suggested by a similar theorem of Chevalley on Lie algebras in characteristic 0) according to which the *derived group* of a representable formal Lie group is essentially *algebraic.* From this it follows also that *simple* formal Lie groups which are not abelian are essentially *algebraic,* and the latter have recently been determined by C. Chevalley [7], who has shown that they are the same as in characteristic 0, namely the groups of the Killing-Cartan classification. To sum up, it seems that a general formal Lie group is essentially built up out of *algebraic* groups and *abelian* formal Lie groups; and, contrary to what might have been expected, the theory of non-commutative formal Lie groups does not exhibit startlingly new features when compared to the classical theory; the radically new phenomena (should one say the "pathology" because they have never been met before?) occur in the theory of *abelian* Lie groups (and in the general case, are confined to the *center* of the group).

There is one additional point, however, which should be duly emphasized: in order to develop the method outlined above, it is first necessary to have at hand the usual tools of group theory, such as subgroups, quotient groups, group of commutators, etc. This might seem at first glance to offer no problem at all, but one must remember that the *set-theoretic* background, which is usually taken for granted (and plays an essential part in the development of the papers [2] and [6] quoted above), simply does not exist in our theory: a "formal Lie group" *is not* a set, has no "elements" nor "subsets", and we are thus denied the use of set-theoretic arguments, at least until we have been able to find substitutes for them by defining anew all the notions which, in the theory of algebraic groups or of Lie algebras, are based on the theory of sets. This is the object of the first two parts of the paper, part III being devoted to the proof of the main results. It is in the definition of these basic notions that the hyperalgebra is particularly useful, for there the set-theoretic notions again become available; however there arise unexpected difficulties, and actually the hardest theorem to prove is that the subgroups of a formal Lie group form a *lattice* (for a convenient definition of "inclusion"), a fact which would hardly need a proof in the classical theories.

I am much indebted to M. Rosenlicht for useful information on algebraic geometry and for many stimulating comments.

2. Preliminaries. We do not recall here the definitions of a formal Lie group G of finite dimension n over a field K, of the hyperalgebra $\mathfrak{G}$ of such a group,[2] of a homomorphism $\boldsymbol{u}$ of G into a formal Lie group G_1 (over the same field K) and of the derived homomorphism $\boldsymbol{u}'$ of $\mathfrak{G}$ into the hyperalgebra $\mathfrak{G}_1$ of G_1 (see [8]); until no. 14, when we speak of a "group", a formal Lie group will always be meant. It will be convenient, when considering a system $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)$ of n indeterminates which intervene in the definition of G, to refer to it as a "generic point" of G; when dealing with several "generic points", $\boldsymbol{x},\boldsymbol{y},\boldsymbol{z},\cdots$, to say that they are "independent" will mean that all the indeterminates in these various systems are distinct from one another. The notation of these systems by boldface characters will prevent any confusion with the usual notion of "generic point". We recall that $\boldsymbol{x}\cdot\boldsymbol{y}$ or $\boldsymbol{xy}$ is an abbreviation for the system $\phi(\boldsymbol{x},\boldsymbol{y})=(\phi_1(\boldsymbol{x},\boldsymbol{y}),\cdots,\phi_n(\boldsymbol{x},\boldsymbol{y}))$ of n formal power series which defines the group law of G; for any system $\gamma=(\gamma_1,\cdots,\gamma_n)$ of n integers $\geqq 0$, $\boldsymbol{x}^\gamma$ is the monomial $x_1^{\gamma_1}\cdots x_n^{\gamma_n}$; if $\boldsymbol{u}=(u_1,\cdots,u_n)$, $\boldsymbol{v}=(v_1,\cdots,v_n)$ are two systems of n power series (without constant terms) in certain indeterminates, $\boldsymbol{uv}$ and $\boldsymbol{u}^\gamma$ will then designate the system of power series (resp. the power series) obtained by substituting u_i for x_i and v_i for y_i $(1\leqq i\leqq n)$ in $\boldsymbol{xy}$ and $\boldsymbol{x}^\gamma$ respectively.

A formal Lie group G over a field K can also be considered as a formal Lie group over any extension L of K; when we do so, we will write it $G_{(L)}$; the necessity of distinguishing these two groups arises from the fact that the notions of homomorphism and of hyperalgebra depend on the ground field. More precisely, any homomorphism of G into $\bar{G}$ is also a homomorphism of $G_{(L)}$ into $\bar{G}_{(L)}$, but not conversely; and the hyperalgebra of $G_{(L)}$ is (as an algebra) obtained by extension to L of the field of scalars of $\mathfrak{G}$, and will accordingly be written $\mathfrak{G}_{(L)}$. We will only consider in this paper the case in which the ground field K is a *perfect* field of characteristic $p>0$.

We keep the notations of [8], except that we write $\mathfrak{S}_{r-1}$ instead of $\mathfrak{S}_r$ for the algebra of left-invariant special semi-derivations of height $\leqq r$; $\mathfrak{S}_{r-1}$ is thus the enveloping algebra of the Lie p-algebra $\mathfrak{g}_{r-1}$ of left-invariant semi-derivations of height $\leqq r-1$. We recall that the identity I and the left-invariant differential operators Z_α (defined by the condition that $Z_\alpha(\boldsymbol{e})=D_\alpha(\boldsymbol{e})$) form a basis for the hyperalgebra $\mathfrak{G}$ over K, which we will call the

---

[2] I will systematically use the convention by which a German capital represents the hyperalgebra of a group represented by the corresponding Latin capital.

LEMMA 1. *If the group law of G is pseudo-canonical, then, for every* $\alpha = \alpha_1\epsilon_1 + \cdots + \alpha_n\epsilon_n \in N^n$, *we have* $Z_\alpha = Z_{\alpha_1\epsilon_1} Z_{\alpha_2\epsilon_2} \cdots Z_{\alpha_n\epsilon_n}$; *furthermore, if* $p^h \leqq \alpha_i < p^{h+1}$, $Z_{\alpha_i\epsilon_i}$ *is an element of the subalgebra of* $\mathfrak{G}$ *generated by* $X_{0i}, X_{1i}, \cdots, X_{hi}$.

Moreover, we have shown in [12, no. 12, th. 2] that any group G of dimension n is isomorphic to a group $\bar{G}$ with pseudo-canonical group law. Actually, the proof of that result yields a "standard process" for the construction of such an isomorphism, which we summarize for future use: starting with the group $G_0 = G$, one defines a sequence (G_r) of groups, and for each r an isomorphism $\boldsymbol{u}_r$ of G_r onto G_{r+1}, such that the following conditions are satisfied. Let (Z_α) be the structural basis of $\mathfrak{G}_r$, and let f be the algebra homomorphism of $\mathfrak{H}_n(K)$ onto $\mathfrak{G}_r$ such that $f(U_{hi}) = X_{hi}$ for all pairs (h, i) $(h \geqq 0, 1 \leqq i \leqq n)$; then we have $f(V_\alpha) = Z_\alpha$ for all indices $\alpha = \alpha_1\epsilon_1 + \cdots + \alpha_n\epsilon_n$ of height $< r$. In general, if we write $f(V_\alpha) = \sum_\lambda b_{\alpha\lambda} Z_\lambda$, we thus see that we have $b_{\alpha\alpha} = 1$ and $b_{\alpha\lambda} = 0$ for $\lambda \neq \alpha$, *for any* $\alpha \in N^n$ *such that* $h(\alpha) < r$ *and for* $\alpha = p^r\epsilon_i$ $(1 \leqq i \leqq n)$. Now, if $\boldsymbol{x}' = (x'_i)$ is a generic point for G_{r+1}, $\boldsymbol{u}^{-1}_r$ is defined by the formulae

$$u^{-1}_{ri}(\boldsymbol{x}') = \sum_\alpha b_{\alpha\epsilon_i} \boldsymbol{x}'^\alpha \qquad (1 \leqq i \leqq n)$$

and the preceding remark shows that, on the right-hand side, we have the term x'_i, all the other terms have a height $\geqq r$, and the monomials $x'^{p^r}_j$ have coefficient 0 $(1 \leqq j \leqq n)$. From which it follows that

$$u_{ri}(\boldsymbol{x}) = x_i + v_{ri}(\boldsymbol{x}) \qquad (1 \leqq i \leqq n) \tag{1}$$

where, in the power series v_{ri} $(1 \leqq i \leqq n)$, all monomials *have a height* $\geqq r$, and there are no monomials $x^{p^r}_j$ $(1 \leqq j \leqq n)$. Having thus defined the isomorphism $\boldsymbol{u}_r$, it follows from the preceding remark that the "infinite product" $\cdots \boldsymbol{u}_r \boldsymbol{u}_{r-1} \cdots \boldsymbol{u}_0$ is meaningful and is an isomorphism of G onto a group $\bar{G}$ with pseudo-canonical group law.

I. Homomorphisms and Subgroups.

4. Homomorphisms. One of our main tools in this paper will be the *homomorphism theorem* [8, th. 6, p. 107]. We recall that, according to that theorem (in which the assumption that K is *perfect* is an essential one), if $\boldsymbol{u}$ is a homomorphism of G into G', it is possible to "change variables" in G and G' (in other words, to replace $\boldsymbol{u}$ by $\boldsymbol{g}\boldsymbol{u}\boldsymbol{f}$, where $\boldsymbol{f}$ and $\boldsymbol{g}$ are isomorphisms) in such a way that

$$(2)\qquad \begin{array}{lll} u_i(x)=x_i & \text{for} & 1\leqq i\leqq r_0 \\ u_i(x)=x^p_i & \text{for} & r_0+1\leqq i\leqq r_0+r_1 \\ \cdots\cdots\cdots\cdots & & \\ u_i(x)=x^{p^t}_i & \text{for} & r_0+\cdots+r_{t-1}+1\leqq i\leqq r_0+\cdots+r_t=\rho \\ u_i(x)=0 & \text{for} & i>\rho. \end{array}$$

To these formulae correspond, for the derived homomorphism $\boldsymbol{u}'$, the formulae

$$(3)\qquad \begin{array}{lll} \boldsymbol{u}'(X_{hi})=X'_{hi} & \text{for} & 1\leqq i\leqq r_0 \\ \boldsymbol{u}'(X_{hi})=X'_{h-1,i} & \text{for} & r_0+1\leqq i\leqq r_0+r_1 \\ \cdots\cdots\cdots\cdots & & \\ \boldsymbol{u}'(X_{hi})=X'_{0i} & \text{for} & r_0+\cdots+r_{h-1}+1\leqq i\leqq r_0+\cdots+r_h \\ \boldsymbol{u}'(X_{hi})=0 & \text{for} & i>r_0+\cdots+r_h \end{array}$$

where we agree to put $r_h=0$ for $h>t$. The integers r_k (some of which may be 0), which we will call the *partial ranks* of $\boldsymbol{u}$, actually depend only on the original homomorphism $\boldsymbol{u}$ and not on the particular isomorphisms f, g which yield the formulae (2); $\rho=r_0+\cdots+r_t$ is the *rank* of $\boldsymbol{u}$, and t (greatest integer for which $r_t\neq 0$) the *height* of $\boldsymbol{u}$. We say that the homomorphism $\boldsymbol{u}$ is *separable* if $t=0$, *inseparable* if $t>0$, *trivially inseparable* if $t>0$, $\rho=r_t$; in that case, $\boldsymbol{u}$ can be written $\boldsymbol{v}\circ\boldsymbol{p}^t$, where $\boldsymbol{v}$ is a separable homomorphism of $G^{(t)}$ into G'. We say that $\boldsymbol{u}$ is *injective* if $\rho=\dim G$, *surjective* if $\rho=\dim G'$; a *monomorphism* (resp. an *epimorphism*) is a homomorphism which is both injective (resp. surjective) *and separable.* From (3) we derive at once the following criterion:

PROPOSITION 1. *In order that a homomorphism $\boldsymbol{u}$ of G into G' be separable, a necessary and sufficient condition is that the image $\boldsymbol{u}'(\mathfrak{g}_0)$ of the Lie algebra of G by the derived homomorphism $\boldsymbol{u}'$ be a Lie subalgebra of dimension ρ of the Lie algebra of G'.*

COROLLARY. *If $\boldsymbol{u}$, $\boldsymbol{v}$ are both monomorphisms* (resp. *both epimorphisms*) *of G into G' and of G' into G'' respectively, then $\boldsymbol{v}\circ\boldsymbol{u}$ is also a monomorphism* (resp. *an epimorphism*).

However, we will see later (no. 21) that $\boldsymbol{v}\circ\boldsymbol{u}$ may well be inseparable even if $\boldsymbol{u}$ and $\boldsymbol{v}$ are separable homomorphisms.

Following M. Rosenlicht [16], we will say that a homomorphism $\boldsymbol{u}$ is an *isogeny* if it is both injective and surjective; an isomorphism is a separable isogeny; an isogeny which is trivially inseparable is obtained by composing an isomorphism with an iterate of the Frobenius homomorphism.

PROPOSITION 2. *If* $\boldsymbol{u}$ *is an isogeny of height* t *of* G *onto* G', *there is a unique isogeny* $\boldsymbol{v}$ *of* G' *onto* $G^{(t)}$ *such that* $\boldsymbol{v}\circ\boldsymbol{u}=\boldsymbol{p}^t$.

We can suppose $\boldsymbol{u}$ is given by (2) with $\rho=n=\dim G=\dim G'$. Let $\phi=(\phi_i)$ and $\psi=(\psi_i)$ be the group laws of G and G' respectively; by definition, we have, for two independent generic points $\boldsymbol{x}=(x_i)$, $\boldsymbol{y}=(y_i)$ of G, the following identities:

$$\begin{aligned}\psi_i(x_1,\cdots,x_{r_0},x^p{}_{r_0+1},\cdots,x^p{}_{r_0+r_1},x^{p^2}{}_{r_0+r_1+1},\cdots,x^{p^t}{}_n;&\\ y_1,\cdots,y_{r_0},y^p{}_{r_0+1},\cdots,y^{p^t}{}_n)=(\phi_i(x_1,\cdots,x_n;y_1,\cdots,y_n))^{p^h}&\end{aligned}\tag{4}$$

for $r_0+\cdots+r_{h-1}+1\leqq i\leqq r_0+\cdots+r_h$, $0\leqq h\leqq t$. Raise both sides of (4) to the power p^{t-h}, and denote by $\phi^{(t)}=(\phi^{(t)}{}_i)$ the group law of $G^{(t)}$; then if we put $x'_i=x^{p^h}{}_i$ for $r_0+\cdots+r_{h-1}+1\leqq i\leqq r_0+\cdots+r_h$, $0\leqq h\leqq t$, the resulting identities can be written

$$\begin{aligned}\phi_i^{(t)}(x'_1{}^{p^t},\cdots,x'^{p^t}{}_{r_0},x'^{p^{t-1}}{}_{r_0+1},\cdots,x'^{p^{t-1}}{}_{r_0+r_1},x'^{p^{t-2}}{}_{r_0+r_1+1},\cdots,x'_n;&\\ y'_1{}^{p^t},\cdots,y'^{p^t}{}_{r_0},y'^{p^{t-1}}{}_{r_0+1},\cdots,y'_n)=(\psi_i(x'_1,\cdots,x'_n;y'_1,\cdots,y'_n))^{p^{t-h}}&\end{aligned}$$

for $r_0+\cdots,+r_{h-1}+1\leqq i\leqq r_0+\cdots+r_h$, $0\leqq h\leqq t$. If we define $v_i(x')$ to be equal to $x'^{p^{t-h}}{}_i$ for $r_0+\cdots+r_{h-1}+1\leqq i\leqq r_0+\cdots+r_h$, $0\leqq h\leqq t$, this shows that $\boldsymbol{v}=(v_i)$ is an isogeny which satisfies the required conditions, and it is obviously unique.

We will say that two groups G, G' are *isogenous* if there exists an isogeny of G onto a group $G'^{(s)}$, where s is a positive or negative integer. This relation is clearly *transitive*, for if $\boldsymbol{u}=(u_i)$ is an isogeny of G onto G', and if $\boldsymbol{u}^{(s)}$ denotes the system of series $u_i^{(s)}$ obtained by raising the coefficients of the u_i to the power p^s, $\boldsymbol{u}^{(s)}$ is clearly an isogeny of $G^{(s)}$ onto $G'^{(s)}$. Moreover Proposition 2 shows that if G is isogenous to G', G' is isogenous to G, for if there is an isogeny of height t of G onto $G'^{(s)}$, there is an isogeny of G' onto $G^{(t-s)}$. In other words, isogeny is an *equivalence relation* between groups of same dimension. It is easy to see that that relation can be defined in the same terms as those used by M. Rosenlicht [16, p. 147] to define isogeny between algebraic groups: namely, G_1 and G_2 are isogenous if and only if there exists a group G_3 and two isogenies of G_3 on G_1 and G_2 respectively. For if there is an isogeny $\boldsymbol{u}$ of G_1 onto $G_2{}^{(s)}$, then we can suppose $s\geqq 0$ (otherwise $\boldsymbol{p}^{-s}\circ\boldsymbol{u}$ is an isogeny of G_1 onto G_2), and then take $G_3=G_1{}^{(-s)}$, the isogenies on G_1 and G_2 being $\boldsymbol{p}^s$ and $\boldsymbol{u}^{(-s)}$ respectively. Conversely, if $\boldsymbol{v}$ and $\boldsymbol{w}$ are isogenies of G_3 on G_1 and G_2, respectively, then by Proposition 2, there is an isogeny $\boldsymbol{u}$ of G_1 onto some $G_3{}^{(t)}$, and $\boldsymbol{w}\circ\boldsymbol{u}^{(t)}$ is an isogeny of G_1 onto $G_2{}^{(t)}$.

5. Subgroups and subhyperalgebras. We slightly modify the formulation of the definition of a subgroup given in [8]: we define a *subgroup of dimension* m of a formal Lie group G of dimension n as a pair (H, f) consisting of a formal Lie group H of dimension m and a *monomorphism* f of H into G. That this definition is essentially the same as that of [8] is seen by remarking that it follows from the homomorphism theorem that there is an isomorphism $\boldsymbol{v}$ of G onto a group $\bar{G}$ and an isomorphism $\boldsymbol{u}$ of a group $\bar{H}$ onto H such that $\boldsymbol{v} \circ f \circ \boldsymbol{u}$ will have the form (2) with $\rho = r_0 = m$; we may say in that case that the subgroup $(\bar{H}, \boldsymbol{v} \circ f \circ \boldsymbol{u})$ of $\bar{G}$ is *typical*, and is *defined by the equations* $x_{m+1} = \cdots = x_n = 0$.

Moreover, we shall *identify* two subgroups (H_1, f_1), (H_2, f_2) of G if there is an isomorphism $\boldsymbol{u}$ of H_1 onto H_2 such that $f_1 = f_2 \circ \boldsymbol{u}$[3]; and we will say that the subgroup (H_1, f_1) is *contained* in the subgroup (H_2, f_2) if there is a monomorphism $\boldsymbol{u}$ of H_1 into H_2 such that $f_1 = f_2 \circ \boldsymbol{u}$.

PROPOSITION 3. *In order that a subgroup* (H_1, f_1) *of* G *be contained in a subgroup* (H_2, f_2), *a necessary and sufficient condition is that if* $\mathfrak{H}_1$, $\mathfrak{H}_2$ *and* $\mathfrak{G}$ *are the hyperalgebras of* H_1, H_2 *and* G, *the subalgebra* $f'_1(\mathfrak{H}_1)$ *of* $\mathfrak{G}$ *be contained in the subalgebra* $f'_2(\mathfrak{H}_2)$.

The condition is obviously necessary. Conversely, suppose it is satisfied, and observe that, from the homomorphism theorem, it follows that a monomorphism $\boldsymbol{u}$ is *characterized* by the fact that $\boldsymbol{u}'$ is *injective*: f'_2 can therefore be considered as an isomorphism of $\mathfrak{H}_2$ onto the subalgebra $f'_2(\mathfrak{H}_2)$ of $\mathfrak{G}$, and in addition we know [9, p. 221] that $(f'_2(Y))^0 = (f'_2 \otimes f'_2)(Y^0)$ for every $Y \in \mathfrak{H}_2$; if $\boldsymbol{s}_2$ is the isomorphism of $f'_2(\mathfrak{H}_2)$ onto $\mathfrak{H}_2$, inverse to f'_2, we have therefore $(\boldsymbol{s}_2(Z))^0 = (\boldsymbol{s}_2 \otimes \boldsymbol{s}_2)(Z^0)$ for every $Z \in f'_2(\mathfrak{H}_2)$. Let $\boldsymbol{r} = \boldsymbol{s}_2 \circ f'_1$; this is an injective homomorphism of $\mathfrak{H}_1$ into $\mathfrak{H}_2$ such that $(\boldsymbol{r}(X))^0 = (\boldsymbol{r} \otimes \boldsymbol{r})(X^0)$ for every $X \in \mathfrak{H}_1$. But that condition implies that $\boldsymbol{r}$ is the derived homomorphism of a monomorphism $\boldsymbol{u}$ of H_1 into H_2 [10, p. 59, prop. 2], and as $f'_1 = f'_2 \circ \boldsymbol{r}$ by definition, we have $f_1 = f_2 \circ \boldsymbol{u}$.

For a subgroup (H, f) of G, we will say that $f'(\mathfrak{H})$ is the *subhyperalgebra* of $\mathfrak{G}$ corresponding to the subgroup; Proposition 3 shows that the subhyperalgebras of $\mathfrak{G}$ thus correspond in a one-to-one manner to subgroups of G. We will now characterize them independently of their origin as images of hyperalgebras:

---

[3] For any formal Lie group G' isomorphic to G and any isomorphism f of G' onto G, the subgroup (G', f) is thus identified to the subgroup $(G, 1)$ of G (where 1 designates the identity isomorphism, defined by the n series x_i $(1 \leq i \leq n)$).

THEOREM 1. *In order that a subalgebra* $\mathfrak{H}$ *of the hyperalgebra* $\mathfrak{G}$ *be a subhyperalgebra, the following conditions are necessary and sufficient:*

1°. *For any* $r\geqq 0$ *and any* $X\in\mathfrak{g}_{r+1}\cap\mathfrak{H}$, $X^0-1\otimes X-X\otimes 1$ *belongs to* $(\mathfrak{s}_r\cap\mathfrak{H})\otimes(\mathfrak{s}_r\cap\mathfrak{H})$.

2°. *For any* $r\geqq 0$, *the algebra* $\mathfrak{s}_r\cap\mathfrak{H}$ *is generated by the Lie p-algebra* $\mathfrak{g}_r\cap\mathfrak{H}$.[4]

3°. *For any element* $X\in\mathfrak{g}_r\cap\mathfrak{H}$, *there is an element* $Y\in\mathfrak{g}_{r+1}\cap\mathfrak{H}$ *such that* $X=\boldsymbol{p}'(Y)$.

It is immediate to see that the conditions are necessary, by considering a *typical* subgroup of G. To prove the conditions are sufficient, consider the Lie p-algebra $\mathfrak{g}_0\cap\mathfrak{H}$; performing if necessary a linear transformation on the indeterminates x_i, we can suppose that the structural basis of $\mathfrak{G}$ is such that the X_{0i} of index $\leqq m$ constitute a basis for $\mathfrak{g}_0\cap\mathfrak{H}$; we denote by J the interval $1\leqq i\leqq m$ in $\boldsymbol{N}$. In order to build up a proof by induction, let us first suppose that G satisfies the following assumption:

(A_r) *The group law of* G *is pseudo-canonical* (no. 3), *and the elements* X_α *such that* $\alpha\in\boldsymbol{N}^J$ *and* $h(\alpha)\leqq r$ *form a basis for* $\mathfrak{s}_r\cap\mathfrak{H}$.

Observe that, owing to Lemma 1, the Z_α such that $\alpha\in\boldsymbol{N}^J$ and $h(\alpha)\leqq r$ also form a basis for $\mathfrak{s}_r\cap\mathfrak{H}$.

From assumption 3°, for every index $i\in J$, there exists in $\mathfrak{g}_{r+1}\cap\mathfrak{H}$ an element $Y_{r+1,i}$ such that $\boldsymbol{p}'(Y_{r+1,i})=X_{ri}$, and we can obviously write $Y_{r+1,i}=X_{r+1,i}+\sum_\lambda c_{r\lambda}Z_\lambda$, where the summation extends over all indices λ of height $h(\lambda)\leqq r$. I claim that $c_{r\lambda}=0$ for all λ which are not in $\boldsymbol{N}^J$ and are different from the ϵ_j $(1\leqq j\leqq n)$. Indeed, if we form the expression $Y^0_{r+1,i}-1\otimes Y_{r+1,i}-Y_{r+1,i}\otimes 1$, which belongs to $(\mathfrak{s}_r\cap\mathfrak{H})\otimes(\mathfrak{s}_r\cap\mathfrak{H})$ by assumption 1°, we obtain

$$\sum_{0<h<p^{r+1}} Z_{h\epsilon_i}\otimes Z_{(p^{r+1}-h)\epsilon_i}+\sum_{\lambda}c_{r\lambda}\Big(\sum_{0<\mu<\lambda}Z_\mu\otimes Z_{\lambda-\mu}\Big)$$

and all the terms $Z_\gamma\otimes Z_\delta$ which intervene in that sum are distinct, hence linearly independent. But from assumption (A_r) it follows that in the preceding sum the only terms $Z_\gamma\otimes Z_\delta$ which can have a coefficient $\neq 0$ are those for which *both* γ and δ belong to $\boldsymbol{N}^J$, whence our assertion.

We can therefore suppose, by subtracting if necessary from $Y_{r+1,i}$ an element of $\mathfrak{s}_r\cap\mathfrak{H}$ (and remembering that by definition $\boldsymbol{p}'(Z_\lambda)=0$ for all the Z_λ which intervene in $Y_{r+1,i}$), that $Y_{r+1,i}=X_{r+1,i}+\sum_{j=1}^{n}a_{ij}X_{0j}$ $(1\leqq i\leqq m)$. Consider now an isomorphism $\boldsymbol{u}$ of G onto a group G' such that we have (writing Z'_α and X'_{hi} for the elements of the structural basis of $\mathfrak{G}'$)

---

[4] I have not been able to determine if condition 1° implies condition 2° or not.

$$(5)\qquad \begin{aligned} \boldsymbol{u}'(X_{hi}) &= X'_{hi} \text{ for } h\leqq r \text{ and for } h=r+1, i\notin J;\\ \boldsymbol{u}'(Y_{r+1,i}) &= X'_{r+1,i} \text{ for } i\in J. \end{aligned}$$

This can be achieved by taking for instance

$$(6)\qquad u_i(\boldsymbol{x})=x_i-\sum_{j=1}^{m}a_{ji}x^{p^{r+1}}_j \qquad \text{for } 1\leqq i\leqq n$$

as it is readily verified. By assumption, there is a homomorphism $\boldsymbol{f}$ of $\mathfrak{H}_n(K)$ onto $\mathfrak{G}$ such that $\boldsymbol{f}(V_\alpha)=Z_\alpha$ for every index; from (5) it follows that we have $\boldsymbol{u}'(\boldsymbol{f}(V_\alpha))=Z'_\alpha$ for all indices α *of height* $\leqq r$. If we denote by $\boldsymbol{v}$ the isomorphism of G' onto a group G'' obtained by the "standard process" of no. 3, it follows at once from the description of that process and from the preceding remark that we can write

$$(7)\qquad v_i(\boldsymbol{x}')=x'_i+w_i(\boldsymbol{x}') \qquad (1\leqq i\leqq n)$$

where in the series w_i, all monomials *have a height* $\geqq r+1$, and there are no monomials $x'^{p^{r+1}}_j$ $(1\leqq j\leqq n)$. Writing X''_{hi} for the elements of the structural basis of $\mathfrak{G}''$, we deduce therefore from (5) that

$$\begin{aligned} \boldsymbol{v}'(\boldsymbol{u}'(X_{hi})) &= X''_{hi} \text{ for } h\leqq r \text{ and for } h=r+1, i\notin J;\\ \boldsymbol{v}'(\boldsymbol{u}'(Y_{r+1,i})) &= X''_{r+1,i} \text{ for } i\in J. \end{aligned}$$

Replacing (for the moment) G by G'', we can therefore suppose from now on that in G the group law is pseudo-canonical, and that we have $Y_{r+1,i}=X_{r+1,i}$ for $i\in J$.

Next we remark that $\mathfrak{g}_{r+1}\cap\mathfrak{H}$ has a basis consisting of the Z_α of height $\leqq r$ such that $\alpha\in\boldsymbol{N}^J$, and of the m elements $X_{r+1,i}$ $(i\in J)$. Indeed, if we consider an arbitrary element $Y=\sum_{i=1}^{n}b_iX_{r+1,i}+\sum_{\lambda}c_\lambda Z_\lambda$ of $\mathfrak{g}_{r+1}\cap\mathfrak{H}$ (summation extended over all the indices λ of height $\leqq r$), and if we express that $Y^0-1\otimes Y-Y\otimes 1$ belongs to $(\mathfrak{z}_r\cap\mathfrak{H})\otimes(\mathfrak{z}_r\cap\mathfrak{H})$, we see at once (using assumption (A_r)) that the only coefficients which can be $\neq 0$ are the b_i for $i\in J$ and the c_λ for which $\lambda\in\boldsymbol{N}^J$. As $\mathfrak{g}_{r+1}\cap\mathfrak{H}$ is a Lie p-algebra, the elements $X^p_{r+1,i}$ and $[X_{r+1,i},X_{r+1,j}]$ (i,j in J) are in $\mathfrak{g}_{r+1}\cap\mathfrak{H}$; using now assumption 2°, we see that the elements X_α of height $\leqq r+1$ and such that $\alpha\in\boldsymbol{N}^J$, form a basis for $\mathfrak{z}_{r+1}\cap\mathfrak{H}$. Due to the fact that the group law is pseudo-canonical, Lemma 1 shows that the Z_α such that $h(\alpha)\leqq r+1$ and $\alpha\in N^J$ also form a basis for $\mathfrak{z}_{r+1}\cap\mathfrak{H}$.

Summing up what we have done, and slightly changing the notations, we have proved the following result: if G_r is a group, in the hyperalgebra $\mathfrak{G}_r$ of which the subalgebra $\mathfrak{H}_r$ verifies the assumptions of Theorem 1 and the assumptions (A_r), then there is an isomorphism $\boldsymbol{g}_r$ mapping G_r onto a group G_{r+1} in such a way that $\mathfrak{H}_{r+1}=\boldsymbol{g}'_r(\mathfrak{H}_r)$ now satisfies the assumptions of Theorem 1 and the assumptions (A_{r+1}). Moreover, $\boldsymbol{g}_r$ being obtained by composing the isomorphisms noted $\boldsymbol{v}$ and $\boldsymbol{u}$ above, we have $g_{ri}(\boldsymbol{x})=x_i+h_{ri}(\boldsymbol{x})$ $(1\leqq i\leqq n)$, where in the power series h_{ri}, all monomials have a height $\geqq r+1$. As usual, we can now therefore consider the "infinite product" $\cdots\boldsymbol{g}_r\boldsymbol{g}_{r-1}\cdots\boldsymbol{g}_0$, with $G_0=G$; this is an isomorphism $\boldsymbol{g}$ of G onto a group G_∞ such that the group law of G_∞ is pseudo-canonical, and $\mathfrak{H}_\infty=\boldsymbol{g}'(\mathfrak{H})$ now satisfies the assumptions of Theorem 1, and assumptions (A_r) for *every* r. This shows that we may suppose that, by a suitable isomorphism, the Z_α such that $\alpha\in N^J$ form a basis for $\mathfrak{H}$; but then property 1° shows that these Z_α constitute the structural basis of a hyperalgebra [10, p. 59, prop. 1] and this ends the proof of Theorem 1.

We may observe here that Theorem 1 obviously implies Theorem 1 of [13], of which we thus obtain an alternate proof.

A similar method enables one to prove

PROPOSITION 4. *Let* $H_1\subset H_2\subset\cdots\subset H_s$ *be a strictly increasing sequence of subgroups*[5] *of* G, *of dimensions* $m_1<m_2<\cdots<m_s\leqq n$; *let* J_k *be the interval* $1\leqq i\leqq m_k$ $(1\leqq k\leqq s)$. *By applying a suitable isomorphism to* G, *it is possible to suppose that the group law of* G *is pseudo-canonical and that, for each* k $(1\leqq k\leqq s)$, *the subgroup* H_k *is typical and defined by the equations* $x_i=0$ *for* $i\notin J_k$.

We only sketch the proof. First, by a linear isomorphism, one can suppose that for each k $(1\leqq k\leqq s)$, the X_{0i} such that $i\in J_k$ form a basis for $\mathfrak{g}_0\cap\mathfrak{H}_k$. Then one builds up an inductive proof by supposing that the group law of G is pseudo-canonical and that for each k $(1\leqq k\leqq s)$ the elements X_α such that $\alpha\in N^{J_k}$ and $h(\alpha)\leqq r$ form a basis for $\mathfrak{z}_r\cap\mathfrak{H}_k$. One then defines the $Y_{r+1,i}$ $(1\leqq i\leqq n)$ such that $Y_{r+1,i}-X_{r+1,i}\in\mathfrak{g}_0$, first for $i\in J_1$ by the condition that $Y_{r+1,i} \in \mathfrak{g}_{r+1} \cap \mathfrak{H}_1$, then for $i \in J_2 - J_1$ by the condition $Y_{r+1,i} \in \mathfrak{g}_{r+1} \cap \mathfrak{H}_2$ etc. We omit the remainder of the proof, which follows very closely that of Theorem 1.

---

[5] From now on, we will most of the time omit the mention of the monomorphism f in the notation of a subgroup (H,f), and simply write it H; we will refer to f as the "natural injection" of H into G. Similarly, when we will speak of the "restriction to H" of a homomorphism $\boldsymbol{u}$ of G into a group G', we mean the homomorphism $\boldsymbol{u}\circ f$ of H into G'; etc.

We define the *dimension* of a subhyperalgebra $\mathfrak{H}$ of $\mathfrak{G}$ as the dimension of the subgroup of G of which $\mathfrak{H}$ is the subhyperalgebra (no confusion can arise with the dimension of $\mathfrak{H}$ as a vector space, which is always infinite); it is equal to the dimension of the Lie algebra $\mathfrak{g}_0 \cap \mathfrak{H}$ over K. If $\mathfrak{H}$, $\mathfrak{H}'$ are two subhyperalgebras of $\mathfrak{G}$, such that $\mathfrak{H} \subset \mathfrak{H}'$, then $\dim \mathfrak{H} \leqq \dim \mathfrak{H}'$, and the relation $\dim \mathfrak{H} = \dim \mathfrak{H}'$ implies $\mathfrak{H} = \mathfrak{H}'$, as follows from Proposition 3. An obvious consequence of these remarks is that the subhyperalgebras of $\mathfrak{G}$ verify *both chain conditions* for the inclusion relation.

It is natural to ask if the subgroups of a formal Lie group (or the corresponding subhyperalgebras) form a *lattice* for the inclusion relation. We will be able to show that such is the case, but only *via* a very indirect argument (no. 17). The difficulties which block a direct approach are the following ones: it is very easy to give examples (for a product G of three additive groups) of subhyperalgebras $\mathfrak{H}_1$, $\mathfrak{H}_2$ of $\mathfrak{G}$ such that $\mathfrak{H}_1 \cap \mathfrak{H}_2$ *is not a subhyperalgebra*; one may ask if the *subalgebra* of $\mathfrak{G}$ generated by $\mathfrak{H}_1 \cup \mathfrak{H}_2$ is a subhyperalgebra; I will prove in no. 9 that such is the case when one of the subgroups H_1, H_2 is normal, but the proof will clearly show the obstacles to the extension of that result (if true) to the general case.

As soon as we have proved that the l. u. b. (resp. g. l. b.) of two subgroups H_1, H_2 exists, we will write it $H_1 \vee H_2$ (resp. $H_1 \wedge H_2$), and use similar notations for the l. u. b. and g. l. b. of subhyperalgebras.

II. Normal Subgroups and Quotient Groups.

6. Inner automorphisms and normal subgroups. Let G be a formal Lie group of dimension n over K; we know [8, p. 88] that there exists a unique system θ of n formal power series $\theta_i(x)$ $(1 \leqq i \leqq n)$ such that $\phi(x, \theta(x)) = \phi(\theta(x), x) = e$. If we write x^{-1} for that system of n power series,[6] we can therefore define, for two independent generic points x, z of G, zxz^{-1} as the system of n power series $\phi_i(\phi(z,x), \theta(z))$; if y is another independent generic point of G, we have $(zxz^{-1})(zyz^{-1}) = z(xy)z^{-1}$ by the usual associativity argument. Let L be a perfect field containing the ring $K[[z]] = K[[z_1, \cdots, z_n]]$ of power series in the z_i with coefficients in K;

---

[6] The relations $(x^{-1})^{-1} = x$, $(xy)^{-1} = y^{-1}x^{-1}$, $u(x^{-1}) = (u(x))^{-1}$ (for a homomorphism u) are proved by the standard arguments.

we can say that the system $\boldsymbol{i}_z(\boldsymbol{x}) = \boldsymbol{z}\boldsymbol{x}\boldsymbol{z}^{-1}$ of n power series in $x_1, \cdots, x_n$, with coefficients in L, defines an *automorphism* of the group $G_{(L)}$, which we will call an *inner automorphism* of $G_{(L)}$ (or of G by abuse of language); its derivative $\boldsymbol{i}'_z$ is an automorphism of the hyperalgebra $\mathfrak{G}_{(L)}$.

More generally, if $\boldsymbol{u}$ is a homomorphism of a group H into G, $\boldsymbol{y}$ a generic point of H and L a perfect field containing $K[[\boldsymbol{y}]]$, the system $\boldsymbol{i}_{\boldsymbol{u}(\boldsymbol{y})}(\boldsymbol{x}) = \boldsymbol{u}(\boldsymbol{y})\boldsymbol{x}(\boldsymbol{u}(\boldsymbol{y}))^{-1}$ of n power series in the x_i, with coefficients in L, defines an automorphism of $G_{(L)}$.

Let $(H, \boldsymbol{f})$ be a subgroup of G, $\mathfrak{H}$ the corresponding subhyperalgebra of $\mathfrak{G}$. We say that $(H, \boldsymbol{f})$ is a *normal subgroup* of G if the subgroup $(H_{(L)}, \boldsymbol{i}_z \circ \boldsymbol{f})$ of $G_{(L)}$ is contained in $(H_{(L)}, \boldsymbol{f})$, in the sense of no. 5; by Proposition 3, an equivalent condition is that $\boldsymbol{i}'_z(\mathfrak{H}) \subset \mathfrak{H}_{(L)}$. If we suppose that $(H, \boldsymbol{f})$ is a *typical* subgroup defined by $x_{m+1} = \cdots = x_n = 0$, then in order that such a subgroup be normal, necessary and sufficient conditions are that in the system $\boldsymbol{i}_z(\boldsymbol{x}) = (h_1(\boldsymbol{x}), \cdots, h_n(\boldsymbol{x}))$ of n power series in the x_i and z_i, the n-m last series be 0.

It is clear that $\boldsymbol{i}'_z(\mathfrak{H}_{(L)}) \subset \mathfrak{H}_{(L)}$, and as these two subhyperalgebras have same dimension over L, we have $\boldsymbol{i}'_z(\mathfrak{H}_{(L)}) = \mathfrak{H}_{(L)}$. We also note that if H is a normal subgroup of G, then, for any perfect extension E of K, $H_{(E)}$ is a normal subgroup of $G_{(E)}$.

7. Kernels and normal subgroups. Let $\boldsymbol{u}$ be a homomorphism of rank ρ of a group G of dimension n into a group G'; if $\boldsymbol{u}$ has the form (2), we have defined in [8, p. 114], the *kernel* of $\boldsymbol{u}$ as the typical subgroup of G, of dimension $n-\rho$, defined by the relations $x_i = 0$ for $i > \rho$. We will first see that this notion is an intrinsic one:

PROPOSITION 5. *The subhyperalgebra $\mathfrak{N}$ of $\mathfrak{G}$ corresponding to the kernel of $\boldsymbol{u}$ is the largest subhyperalgebra $\mathfrak{H}$ such that $\boldsymbol{u}'(\mathfrak{H}) = \{0\}$.*

As $\boldsymbol{u}'(\mathfrak{N}) = \{0\}$, it is equivalent to prove that if $\boldsymbol{u}'(\mathfrak{H}) = \{0\}$, then $\mathfrak{H} \subset \mathfrak{N}$. Let us observe that, from (3), it follows that each X'_{hi} is of the form $\boldsymbol{u}'(X_{ki})$ for a *unique* index k; let us order the factors X'_{hi} in the X'_λ in the same order as the corresponding factors X_{ki} have in the products X_α; then those of the $\boldsymbol{u}'(X_\alpha)$ which are not 0 are *distinct* elements X'_λ, hence linearly independent. We prove first that $\mathfrak{H} \cap \mathfrak{g}_0 \subset \mathfrak{N} \cap \mathfrak{g}_0$; indeed, let us suppose there is in $\mathfrak{H} \cap \mathfrak{g}_0$ an element $\sum_{i=1}^{n} c_i X_{0i}$ with at least one of the c_i of index $i \leqq \rho$ being $\neq 0$. As $\mathfrak{H}$ is a subhyperalgebra, condition 3° of Theorem 1 shows that there exists in $\mathfrak{H}$ an element of the form $Y = \sum_{i=1}^{n} c^{p^t}_i X_{ti} + \sum_\lambda d_\lambda X_\lambda$

the summation being extended over indices of height $< t$ and such that $\boldsymbol{p}'^{t}(X_\lambda) = 0$. If we now observe that by (3), none of the $\boldsymbol{u}'(X_{ti})$ with $i \leqq \rho$ is 0, it follows from the preceding remark that we cannot have $\boldsymbol{u}'(Y) = 0$, contradicting the hypothesis. From that result and conditions 2° of Theorem 1 it follows that $\mathfrak{H} \cap \mathfrak{s}_0 \subset \mathfrak{N} \cap \mathfrak{s}_0$. Suppose now that we have proved that $\mathfrak{s}_r \cap \mathfrak{H} \subset \mathfrak{s}_r \cap \mathfrak{N}$. From the argument in the beginning of the proof of Theorem 1 (based on condition 1°), we see that any element of $\mathfrak{g}_{r+1} \cap \mathfrak{H}$ can be written $Z + \sum_{i=1}^{n} c_i X_{0i}$, with $Z \in \mathfrak{N} \cap \mathfrak{g}_{r+1}$; then $\mathfrak{H}$ also contains an element $Y = \sum_{i=1}^{n} c^{p^t}_i X_{ti} + T + \sum_\lambda d_\lambda X_\lambda$, with $T \in \mathfrak{N}$ and $\boldsymbol{p}'^{t}(X_\lambda) = 0$ for all indices λ in the summation. If one of the c_i of index $\leqq \rho$ was not 0, we would then get $\boldsymbol{u}'(Y) \neq 0$ as above, contradicting again the hypothesis. Therefore $\mathfrak{g}_{r+1} \cap \mathfrak{H} \subset \mathfrak{g}_{r+1} \cap \mathfrak{N}$, hence $\mathfrak{s}_{r+1} \cap \mathfrak{H} \subset \mathfrak{s}_{r+1} \cap \mathfrak{N}$ by condition 2° of Theorem 1, and Proposition 5 is thus proved by induction on r.

THEOREM 2. *Let (N, f) be a subgroup of G, $\mathfrak{N}$ the corresponding sub-hyperalgebra of $\mathfrak{G}$. The following properties are equivalent:*

a) *$(N, \boldsymbol{f})$ is a normal subgroup;*

b) *the left (or right) ideal generated in $\mathfrak{G}$ by $\mathfrak{N}^+$ is a two-sided ideal;*

c) *$(N, \boldsymbol{f})$ is the kernel of an epimorphism;*

d) *$(N, \boldsymbol{f})$ is the kernel of a homomorphism.*

It is clear that c) implies d); condition d) implies a), for if $\boldsymbol{u}(\boldsymbol{f}(\boldsymbol{y})) = \boldsymbol{e}'$ for a homomorphism $\boldsymbol{u}$ of G into G' ($\boldsymbol{y}$ generic point of N), we also have, for a generic point $\boldsymbol{z}$ of G independent of $\boldsymbol{y}$, $\boldsymbol{u}(\boldsymbol{z}\boldsymbol{f}(\boldsymbol{y})\boldsymbol{z}^{-1}) = \boldsymbol{u}(\boldsymbol{z})\boldsymbol{u}(\boldsymbol{f}(\boldsymbol{y}))(\boldsymbol{u}(\boldsymbol{z}))^{-1} = \boldsymbol{e}'$, hence by Proposition 5, the subgroup $(N_{(L)}, \boldsymbol{i}_{\boldsymbol{z}} \circ \boldsymbol{f})$ is contained in $(N_{(L)}, \boldsymbol{f})$, which proves that $(N, \boldsymbol{f})$ is normal.

To prove that a) implies b), we can suppose that the group law of G is pseudo-canonical and that N is a typical subgroup defined by the relations $x_1 = \cdots = x_m = 0$; we will denote by I the interval $1 \leqq i \leqq m$, by J the interval $m + 1 \leqq i \leqq n$. Let $\boldsymbol{y} = (y_{m+1}, \cdots, y_n)$; then $\boldsymbol{f}(\boldsymbol{y}) = (0, \cdots, 0, y_{m+1}, \cdots, y_n)$, and if, for simplicity's sake, we write $\boldsymbol{z}^{-1}\boldsymbol{f}(\boldsymbol{y})\boldsymbol{z} = \boldsymbol{h}(\boldsymbol{y}, \boldsymbol{z})$, we have by assumption $\boldsymbol{h}(\boldsymbol{y}, \boldsymbol{z}) = (0, \cdots, 0, h_{m+1}(\boldsymbol{y}, \boldsymbol{z}), \cdots, h_n(\boldsymbol{y}, \boldsymbol{z}))$. By definition, $\boldsymbol{f}(\boldsymbol{y})\boldsymbol{z} = \boldsymbol{z}\boldsymbol{h}(\boldsymbol{y}, \boldsymbol{z})$; remembering that $(\boldsymbol{\phi}(\boldsymbol{x}, \boldsymbol{z}))^\gamma = \sum_{\alpha,\beta} d_{\alpha\beta\gamma} \boldsymbol{x}^\alpha \boldsymbol{z}^\beta$ for two independent generic points $\boldsymbol{x}, \boldsymbol{z}$ of G, we obtain, for any index γ

$$\sum_{\alpha,\beta} d_{\alpha\beta\gamma} (\boldsymbol{f}(\boldsymbol{y}))^\alpha \boldsymbol{z}^\beta = \sum_{\lambda,\mu} d_{\lambda\mu\gamma} \boldsymbol{z}^\lambda (\boldsymbol{h}(\boldsymbol{y}, \boldsymbol{z}))^\mu. \tag{8}$$

Now $(\boldsymbol{f}(\boldsymbol{y}))^\alpha = 0$ unless $\alpha \in \boldsymbol{N}^J$, and similarly $(\boldsymbol{h}(\boldsymbol{y}, \boldsymbol{z}))^\mu = 0$ unless

$\mu \in \boldsymbol{N}^J$. Let α be an arbitrary index in $\boldsymbol{N}^J$, and β an arbitrary index in $\boldsymbol{N}^I$, and let us identify in (8) the unique monomial $d_{\alpha\beta\gamma}(\boldsymbol{f}(\boldsymbol{y}))^\alpha \boldsymbol{z}^\beta$ to the sum of the monomials of same degrees in the y_i and z_j on the right hand side. It is clear that such terms can only come from products $\boldsymbol{z}^\lambda(\boldsymbol{h}(\boldsymbol{y},\boldsymbol{z}))^\mu$ such that $\lambda \in \boldsymbol{N}^I$; hence, we can write

$$d_{\alpha\beta\gamma} = \sum_{\lambda,\mu} a_{\lambda\mu} d_{\lambda\mu\gamma} \tag{9}$$

where on the right hand side, the summation extends only over pairs (λ,μ) *such that* $\lambda \in \boldsymbol{N}^I$ *and* $\mu \in \boldsymbol{N}^J$. But from Lemma 1 it follows that under those conditions $Z_\lambda Z_\mu = Z_{\lambda+\mu}$, hence $d_{\lambda\mu\gamma} = 0$ except if $\gamma = \lambda + \mu$, and such a decomposition of an index γ in a sum of $\lambda \in \boldsymbol{N}^I$ and $\mu \in \boldsymbol{N}^J$ is unique, hence $d_{\alpha\beta\gamma} = a_{\lambda\mu} d_{\lambda\mu\gamma}$. On the other hand, if $\alpha \neq 0$ in $\boldsymbol{N}^J$, then we must have $\mu \neq 0$, otherwise the term $\boldsymbol{z}^\lambda$ cannot contain any y_j. We conclude that if $\alpha \in \boldsymbol{N}^J$, $\beta \in \boldsymbol{N}^I$ and $\alpha \neq 0$, then $d_{\alpha\beta\gamma} = 0$ *unless* $\gamma = \lambda + \mu$ *with* $\lambda \in \boldsymbol{N}^I$, $\mu \in \boldsymbol{N}^J$ *and* $\mu \neq 0$.

Now from Lemma 1 it is clear that the left ideal of $\mathfrak{G}$ generated by the subalgebra $\mathfrak{N}^+$ has as a basis over K the elements $Z_{\lambda+\mu}$ with $\lambda \in \boldsymbol{N}^I$, $\mu \in \boldsymbol{N}^J$ and $\mu \neq 0$. As $Z_\alpha Z_\beta = \sum_\gamma d_{\alpha\beta\gamma} Z_\gamma$, the preceding result shows that the right ideal generated by the subalgebra $\mathfrak{N}^+$ is contained in the left ideal generated by that subalgebra, in other words the latter is a two-sided ideal. A similar argument, applied to the group opposite to G, proves that the right ideal generated by $\mathfrak{N}^+$ is the same two-sided ideal as the left ideal generated by $\mathfrak{N}^+$.

Finally, to prove that b) implies c), consider (under the same assumptions regarding the group law of G and the typical form of N) the two-sided ideal $\mathfrak{a}$ generated by $\mathfrak{N}^+$, which has, as we have seen, the $Z_{\lambda+\mu}$ with $\lambda \in \boldsymbol{N}^I$, $\mu \in \boldsymbol{N}^J$ and $\mu \neq 0$, as a basis over K; the elements Z_λ such that $\lambda \in \boldsymbol{N}^I$ span therefore a supplementary subspace to $\mathfrak{a}$ in $\mathfrak{G}$. If $\boldsymbol{s}$ is the natural mapping of $\mathfrak{G}$ onto $\mathfrak{G}/\mathfrak{a} = \mathfrak{G}'$, the elements $\bar{Z}_\lambda = \boldsymbol{s}(Z_\lambda)$ with $\lambda \in \boldsymbol{N}^I$ thus constitute a basis for $\mathfrak{G}'$; furthermore, we have

$$(\boldsymbol{s} \otimes \boldsymbol{s})(Z^0{}_\lambda) = \sum_{0 \leqq \nu \leqq \lambda} \boldsymbol{s}(Z_\nu) \otimes \boldsymbol{s}(Z_{\lambda-\nu})$$

hence $(\boldsymbol{s} \otimes \boldsymbol{s})(Z^0{}_\lambda) = 0$ unless $\lambda \in \boldsymbol{N}^I$. This proves that the image of $\mathfrak{G}'$ into $\mathfrak{G}' \otimes \mathfrak{G}'$ by the linear mapping which to each $\bar{Z}_\lambda$ associates $\bar{Z}^0{}_\lambda = \sum_{0 \leqq \nu \leqq \lambda} \bar{Z}_\nu \otimes \bar{Z}_{\lambda-\nu}$ $(\lambda \in \boldsymbol{N}^I)$ is the subalgebra $\mathfrak{G}'^0 = (\boldsymbol{s} \otimes \boldsymbol{s})(\mathfrak{G}^0)$. Moreover, it is clear that the $\bar{Z}_\lambda$ with $\lambda \neq 0$ constitute a basis for a two-sided ideal of $\mathfrak{G}'$, and the $\bar{Z}_\lambda$ of height $h(\lambda) \leqq r$ a basis of a subalgebra of $\mathfrak{G}'$. Applying Proposition 1 of [10, p. 59], we see that $(\bar{Z}_\lambda)_{\lambda \in \boldsymbol{N}^I}$ is a structural basis for a well determined structure of hyperalgebra on $\mathfrak{G}'$. We will say that the corresponding formal Lie group of dimension n-m is the *quotient group* of G by N, and write it G/N[7]; $\boldsymbol{s}$ is then the derived mapping of an *epimorphism* $\boldsymbol{g}$ of G onto G/N, having kernel N, and which we will call the *natural mapping* of G onto G/N. This concludes the proof of Theorem 2.

We will say that the two-sided ideal $\mathfrak{a}$ generated by $\mathfrak{N}^+$ (which is also the right and the left ideal generated by $\mathfrak{N}^+$) is the *normal ideal* corresponding to N.

The following results are immediate consequences of Theorem 2:

COROLLARY 1. *If N is a normal subgroup of G, $\mathfrak{g}_0 \cap \mathfrak{N}$ is a p-ideal in $\mathfrak{g}_0$, and $\mathfrak{g}_0/(\mathfrak{g}_0 \cap \mathfrak{N})$ is isomorphic to the Lie algebra of G/N.*

COROLLARY 2. *If N is a normal subgroup of G, then, for any perfect extension L of K, $(G/N)_{(L)}$ is identified to $G_{(L)}/N_{(L)}$.*

COROLLARY 3. *If L is a perfect extension of K, and $\mathfrak{a}$ a normal ideal corresponding to a normal subgroup N of G, then the vector space $\mathfrak{a}_{(L)}$ generated by $\mathfrak{a}$ in $\mathfrak{G}_{(L)}$ is the normal ideal corresponding to the normal subgroup $N_{(L)}$ of $G_{(L)}$.*

Let now $\boldsymbol{u}$ be a homomorphism of G into a group G'', having N as its kernel, and reduced to the form (2); we have $\boldsymbol{u}'(Z_\lambda) = 0$ except for $\lambda \in \boldsymbol{N}^I$ and therefore, for λ and μ in $\boldsymbol{N}^I$,

$$\boldsymbol{u}'(Z_\lambda)\boldsymbol{u}'(Z_\mu) = \sum_\nu d_{\lambda\mu\nu}\boldsymbol{u}'(Z_\nu) \qquad (\nu \in \boldsymbol{N}^I). \tag{10}$$

On the other hand, the definition of the $\bar{Z}_\lambda$ yields

$$\bar{Z}_\lambda \bar{Z}_\mu = \sum_\nu d_{\lambda\mu\nu}\bar{Z}_\nu \qquad (\nu \in \boldsymbol{N}^I). \tag{11}$$

Observe that, from the homomorphism theorem, it follows that $\boldsymbol{u}'(\mathfrak{G}) = \mathfrak{L}$ is a subhyperalgebra of $\mathfrak{G}''$. Let $\boldsymbol{t}$ be the linear mapping of $\mathfrak{G}'$ into $\mathfrak{L}$ defined by $\boldsymbol{t}(\bar{Z}_\lambda) = \boldsymbol{u}'(Z_\lambda)$ $(\lambda \in \boldsymbol{N}^I)$; then we have, by the preceding definitions

$$(\boldsymbol{t} \otimes \boldsymbol{t})(\bar{Z}^0{}_\lambda) = \sum_{0 \leqq \nu \leqq \lambda} \boldsymbol{u}'(Z_\nu) \otimes \boldsymbol{u}'(Z_{\lambda-\nu}) = (\boldsymbol{u}' \otimes \boldsymbol{u}')(Z^0{}_\lambda) \in \mathfrak{L} \otimes \mathfrak{L}$$

and on the other hand it follows from (10) and (11) that $\boldsymbol{t}$ is a homomorphism of $\mathfrak{G}'$ into $\mathfrak{L}$; therefore [10, p. 59, prop. 2] $\boldsymbol{t}$ is the derivative of a homomorphism $\boldsymbol{v}$ of G/N onto a group L of hyperalgebra $\mathfrak{L}$. Moreover, there is a monomorphism $\boldsymbol{f}$ of L into G'' and G/N and L have the same dimension, hence $\boldsymbol{v}$ is an isogeny; in other words:

---

[7] Strictly speaking, this group is thus only defined when the group law of G is pseudo-canonical and N is a typical normal subgroup. By abuse of language, we will designate by G/N any formal Lie group isomorphic to G'/N', where G' is a group with pseudo-canonical group law, isomorphic to G by an isomorphism which transforms N into a normal typical subgroup N'.

PROPOSITION 6. *Any homomorphism* $\boldsymbol{u}$ *of* G *into* G'', *of kernel* N, *can be decomposed as* $\boldsymbol{f}\circ\boldsymbol{v}\circ\boldsymbol{g}$, *where* $\boldsymbol{g}$ *is the natural epimorphism of* G *onto* G/N, $\boldsymbol{v}$ *an isogeny of* G/N *onto a group* L, *and* $\boldsymbol{f}$ *a monomorphism of* L *into* G''.

8. Direct and inverse images of subgroups. We have just observed that if $\boldsymbol{u}$ is a homomorphism of G into G', $\boldsymbol{u}'(\mathfrak{G})$ is a subhyperalgebra of $\mathfrak{G}'$. More generally, it follows that if $(H,\boldsymbol{f})$ is a subgroup of G, $\boldsymbol{u}'(\boldsymbol{f}'(\mathfrak{H}))$ is a subhyperalgebra of $\mathfrak{G}'$, since $\boldsymbol{u}\circ\boldsymbol{f}$ is a homomorphism of H into G'; we will say that the corresponding subgroup of G' is the *direct image* of the subgroup $(H,\boldsymbol{f})$ of G by $\boldsymbol{u}$, and we will write it $\boldsymbol{u}(H)$ by abuse of language when we drop the monomorphism $\boldsymbol{f}$ in the notation of a subgroup of G.

PROPOSITION 7. *If* $\boldsymbol{u}$ *is an isogeny of a group* G *onto a group* G', *the mapping* $H\rightarrow\boldsymbol{u}(H)$ *is a bijection of the set of subgroups* (resp. *normal subgroups*) *of* G *onto the set of subgroups* (resp. *normal subgroups*) *of* G'.

Consider first the case in which $G'=G^{(t)}$ and $\boldsymbol{u}=\boldsymbol{p}^t$; then it is clear that $\boldsymbol{u}(H)=H^{(t)}$ for any subgroup H of G, as it is immediately seen when H is taken as typical subgroup; Proposition 7 is just obvious in that case. If now $\boldsymbol{u}$ is any isogeny, there is an isogeny $\boldsymbol{v}$ of G' onto some $G^{(t)}$ such that $\boldsymbol{v}\circ\boldsymbol{u}=\boldsymbol{p}^t$ (Proposition 2), and as $\boldsymbol{u}^{(t)}\circ\boldsymbol{v}=\boldsymbol{p}^t$, the result follows at once.

PROPOSITION 8. *Let* $\boldsymbol{u}$ *be a surjective homomorphism of* G *onto* G'. *For any subgroup* H' *of* G', *there is a largest subgroup* H *of* G *such that* $\boldsymbol{u}(H)\subset H'$; H *is the unique subgroup of* G *containing the kernel* N *of* $\boldsymbol{u}$ *and such that* $\boldsymbol{u}(H)=H'$, *and we have* $\dim H=\dim N+\dim H'$.

It is clear that if there is a largest subgroup H of G such that $\boldsymbol{u}(H)\subset H'$, it must contain N; for any subgroup F of G such that $N\subset F\subset H$, N is then the kernel of the restriction of $\boldsymbol{u}$ to F, and we have, by the homomorphism theorem, $\dim F=\dim N+\dim\boldsymbol{u}(F)$; the proposition will therefore be proved as soon as we establish the existence of a subgroup $H\supset N$ of G such that $\boldsymbol{u}(H)=H'$, and the fact that H is the largest of the subgroups F for which $\boldsymbol{u}(F)\subset H'$.

By Proposition 6, we can write $\boldsymbol{u}=\boldsymbol{v}\circ\boldsymbol{w}$, where $\boldsymbol{w}$ is an epimorphism and $\boldsymbol{v}$ an isogeny; using Proposition 7, we are immediately reduced to the case in which $\boldsymbol{u}$ is an *epimorphism*. Suppose $\dim G=n$, $\dim G'=m\leqq n$, and (using the homomorphism theorem) suppose $\boldsymbol{u}$ is defined by $u_i(\boldsymbol{x}) = x_i$ for $1 \leqq i \leqq m$, $u_i(\boldsymbol{x}) = 0$ for $m+1 \leqq i \leqq n$. We can change variables in G', by an isomorphism $\bar{x}'_i = f_i(x'_1, \cdots, x'_m)$ $(1 \leqq i \leqq m)$ so that H' will be transformed into a typical subgroup defined by $\bar{x}'_i = 0$ for $1 \leqq i \leqq q \leqq m$. If we also change variables in G by $\bar{x}_i = f_i(x_1, \cdots, x_m)$ for $1 \leqq i \leqq m$, $\bar{x}_i = x_i$ for $m+1 \leqq i \leqq n$, then the epimorphism $\boldsymbol{u}$ corresponding to $\boldsymbol{u}$ will again be defined by $\bar{u}_i(\boldsymbol{x}) = \bar{x}_i$ for $1 \leqq i \leqq m$, $\bar{u}_i(\boldsymbol{x}) = 0$ for $m+1 \leqq i \leqq n$. We can therefore suppose that H' was already a typical subgroup of G' defined by $x'_i = 0$ for $1 \leqq i \leqq q$. I claim that the relations $x_i = 0$ for $1 \leqq i \leqq q$ define a typical subgroup H of G, which then obviously contains N and is such that $\boldsymbol{u}(H) = H'$. We have to show that

$$\phi_j(0, \cdots, 0, x_{q+1}, \cdots, x_n, 0, \cdots, 0, y_{q+1}, \cdots, y_n) = 0 \text{ for } j \leqq q.$$

But by assumption we have

$$\phi'_j(0, \cdots, 0, x'_{q+1}, \cdots, x'_m, 0, \cdots, 0, y'_{q+1}, \cdots, y'_m) = 0 \text{ for } j \leqq q.$$

Now, by definition of a homomorphism, we have

$$\phi'_j(x_1, \cdots, x_m, y_1, \cdots, y_m) = \phi_j(x_1, \cdots, x_n, y_1, \cdots, y_n) \text{ for } 1 \leqq j \leqq m;$$

substituting 0 to the x_k and y_k of index $k \leqq q$ in those identities for $1 \leqq j \leqq q$ yields the desired result.

It remains to prove that if a subhyperalgebra $\mathfrak{F}$ of $\mathfrak{G}$ is such that $\boldsymbol{u}'(\mathfrak{F}) \subset \mathfrak{H}'$, then $\mathfrak{F} \subset \mathfrak{H}$. First we have $\boldsymbol{u}'(\mathfrak{F} \cap \mathfrak{g}_0) \subset \mathfrak{H}' \cap \mathfrak{g}'_0$; as $\boldsymbol{u}'(X_{0i}) = X'_{0i}$ for $1 \leqq i \leqq m$, $\boldsymbol{u}'(X_{0i}) = 0$ for $m+1 \leqq i \leqq n$, this shows that $\mathfrak{F} \cap \mathfrak{g}_0 \subset \mathfrak{H} \cap \mathfrak{g}_0$, hence $\mathfrak{F} \cap \mathfrak{s}_0 \subset \mathfrak{H} \cap \mathfrak{s}_0$. Suppose we have proved that $\mathfrak{F} \cap \mathfrak{s}_r \subset \mathfrak{H} \cap \mathfrak{s}_r$; by the argument at the beginning of the proof of Theorem 1, any element of $\mathfrak{F} \cap \mathfrak{g}_{r+1}$ can then be written $Z + \sum_{i=1}^{n} c_i X_{0i}$, with $Z \in \mathfrak{H} \cap \mathfrak{g}_{r+1}$; as $\boldsymbol{u}'(Z) \in \mathfrak{H}'$, we must have $c_i = 0$ for $1 \leqq i \leqq q$, hence $\sum_{i=1}^{n} c_i X_{0i} \in \mathfrak{H}$, which proves that $\mathfrak{F} \cap \mathfrak{g}_{r+1} \subset \mathfrak{H} \cap \mathfrak{g}_{r+1}$, hence $\mathfrak{F} \cap \mathfrak{s}_{r+1} \subset \mathfrak{H} \cap \mathfrak{s}_{r+1}$ (by condition 2° of Theorem 1), which ends the proof.

We will write as usual $H = \boldsymbol{u}^{-1}(H')$, and say that H is the *inverse image of* H' by $\boldsymbol{u}$.

COROLLARY 1. *If* $\boldsymbol{u}$ *is a surjective homomorphism of* G *onto* G', $\boldsymbol{v}$ *a surjective homomorphism of* G' *onto* G'' *and* $\boldsymbol{w} = \boldsymbol{v} \circ \boldsymbol{u}$, *then, for any subgroup* H'' *of* G'', $\boldsymbol{w}^{-1}(H'') = \boldsymbol{u}^{-1}(\boldsymbol{v}^{-1}(H''))$.

For if $H = \boldsymbol{u}^{-1}(\boldsymbol{v}^{-1}(H''))$ we have $\boldsymbol{w}(H) = H''$ by Proposition 8; on the other hand if N' is the kernel of $\boldsymbol{v}$, $\boldsymbol{u}^{-1}(N')$ is the kernel of $\boldsymbol{w}$, for the relation $\boldsymbol{v}(\boldsymbol{u}(F))=\{e''\}$ implies $\boldsymbol{u}(F)\subset N'$ by Proposition 5 for a subgroup F of G, hence $F\subset \boldsymbol{u}^{-1}(N')$, and conversely $\boldsymbol{v}(\boldsymbol{u}(\boldsymbol{u}^{-1}(N')))=\boldsymbol{v}(N')=\{e''\}$. As $N'\subset \boldsymbol{v}^{-1}(H'')$, we have $\boldsymbol{u}^{-1}(N')\subset \boldsymbol{u}^{-1}(\boldsymbol{v}^{-1}(H''))$, and Proposition 8 shows that $H=\boldsymbol{w}^{-1}(H'')$.

COROLLARY 2. *If L is a perfect extension of K, $\boldsymbol{u}^{-1}(H'_{(L)})$ is identical to $(\boldsymbol{u}^{-1}(H'))_{(L)}$.*

For if $H=\boldsymbol{u}^{-1}(H')$, $\boldsymbol{u}(H_{(L)})=H'_{(L)}$, and $H_{(L)}$ contains the kernel $N_{(L)}$ of $\boldsymbol{u}$ (considered as homomorphism of $G_{(L)}$ onto $G'_{(L)}$).

If the homomorphism $\boldsymbol{u}$ is not surjective, we can still prove the existence of a largest subgroup H of G such that $\boldsymbol{u}(H)\subset H'$ as soon as we have proved the g.l.b. $H'\wedge \boldsymbol{u}(G)$ exists; for the relation $\boldsymbol{u}(H)\subset H'$ is then equivalent to $\boldsymbol{u}(H)\subset H'\wedge \boldsymbol{u}(G)$, and considering $\boldsymbol{u}$ as a surjective homomorphism of G onto $\boldsymbol{u}(G)$, we need only take $H=\boldsymbol{u}^{-1}(H'\wedge \boldsymbol{u}(G))$.

9. Lattice properties of normal subgroups.

PROPOSITION 9. *Let H be a subgroup of G, N a normal subgroup of G. Then there is a* g.l.b. $H\wedge N$ *and a* l.u.b. $H\vee N$ *of these two subgroups. If g is the natural epimorphism of G onto G/N, $H\wedge N$ is the kernel of the restriction of g to H, and $H\vee N=g^{-1}(g(H))$.*

The fact that the kernel of the restriction of g to H is $H\wedge N$ follows from Proposition 5. On the other hand, if a subgroup F of G contains both H and N, we have $g(F)\supset g(H)$, hence $g^{-1}(g(F))\supset g^{-1}(g(H))$. But by Proposition 8 $F=g^{-1}(g(F))$, which proves that $g^{-1}(g(H))=H\vee N$.

COROLLARY 1. *For any perfect extension L of K,*

$$H_{(L)}\wedge N_{(L)}=(H\wedge N)_{(L)} \text{ and } H_{(L)}\vee N_{(L)}=(H\vee N)_{(L)}.$$

It is clear that $(H\wedge N)_{(L)}$ is the kernel of the restriction of g to $H_{(L)}$; on the other hand, from corollary 2 to Proposition 8 we have $(g^{-1}(g(H)))_{(L)}=g^{-1}((g(H))_{(L)})$, and consideration of the subhyperalgebras shows that $(g(H))_{(L)}=g(H_{(L)})$.

COROLLARY 2. *If N_1, N_2 are two normal subgroups of G, $N_1\wedge N_2$ and $N_1\vee N_2$ are normal in G.*

Let $\boldsymbol{z}$ be a generic point of G, and L a perfect field containing $K[[z_1,\cdots,z_n]]$; then $\boldsymbol{i}_z((N_1\wedge N_2)_{(L)})\subset \boldsymbol{i}_z(N_{1(L)})=N_{1(L)}$ and similarly $\boldsymbol{i}_z((N_1\wedge N_2)_{(L)})\subset N_{2(L)}$, hence

$$\boldsymbol{i}_z((N_1\wedge N_2)_{(L)})\subset N_{1(L)}\wedge N_{2(L)}=(N_1\wedge N_2)_{(L)},$$

which shows $N_1 \wedge N_2$ is normal; on the other hand $N_{1(L)} = \boldsymbol{i}_s(N_{1(L)}) \subset \boldsymbol{i}_s((N_1 \vee N_2)_{(L)})$ and similarly $N_{2(L)} \subset \boldsymbol{i}_s((N_1 \vee N_2)_{(L)})$, hence $(N_1 \vee N_2)_{(L)} \subset \boldsymbol{i}_s((N_1 \vee N_2)_{(L)})$ and as these two groups have same dimension, they coincide, which proves $N_1 \vee N_2$ is normal in G.

As mentioned above, even if N_1 and N_2 are normal subgroups, $\mathfrak{N}_1 \cap \mathfrak{N}_2$ will not in general be a subhyperalgebra. But we have the surprisingly simple:

THEOREM 3. *If H is a subgroup of G, N a normal subgroup of G, then the subalgebra of $\mathfrak{G}$ generated by $\mathfrak{H} \cup \mathfrak{N}$ is the subhyperalgebra corresponding to $H \vee N$.*

We consider, for each $r \geqq 0$, the subalgebra $\mathfrak{t}_r$ of $\mathfrak{s}_r$ generated by the union of $\mathfrak{s}_r \cap \mathfrak{H}$ and $\mathfrak{s}_r \cap \mathfrak{N}$, and the *Lie-p-algebra* $\mathfrak{m}_r$ generated by the union of $\mathfrak{t}_{r-1}$, $\mathfrak{g}_r \cap \mathfrak{H}$ and $\mathfrak{g}_r \cap \mathfrak{N}$. It is clear that $\mathfrak{t}_r$ is the subalgebra generated by $\mathfrak{m}_r$, by condition 2° of Theorem 1.

Next, consider the increasing sequence of sub-Lie-p-algebras $\mathfrak{m}_r \cap \mathfrak{g}_0$. It is a stationary sequence, in other words there is a smallest integer t such that $\mathfrak{m}_{r+1} \cap \mathfrak{g}_0 = \mathfrak{m}_r \cap \mathfrak{g}_0$ for $r \geqq t$. By a linear isomorphism, we can suppose that the basis $(X_{0i})_{1 \leqq i \leqq n}$ of $\mathfrak{g}_0$ is such that there is an increasing sequence of intervals $I = J_{-1} \subset J_0 \subset J_1 \subset \cdots \subset J_t = J_{t+1} = \cdots$ having the property that the X_{0i} with $i \in I$ form a basis for $\mathfrak{g}_0 \cap \mathfrak{N}$, the X_{0i} such that $i \in J_r$ a basis for $\mathfrak{m}_r \cap \mathfrak{g}_0$ for each value of $r \geqq 0$. As $\mathfrak{g}_0 \cap \mathfrak{N}$ is a p-ideal in the Lie algebra $\mathfrak{g}_0$, it is immediately verified that $\mathfrak{m}_0 = (\mathfrak{g}_0 \cap \mathfrak{N}) + (\mathfrak{g}_0 \cap \mathfrak{H})$.

As a basis for an inductive argument, we will now suppose that G verifies the following conditions:

(B_r) *The group law of G is pseudo-canonical and the basis (X_α) of $\mathfrak{G}$ is such that:*

a) *The X_α for which $h(\alpha) \leqq r$ and $\alpha \in N^I$ form a basis for $\mathfrak{s}_r \cap \mathfrak{N}$.*

b) *The algebra $\mathfrak{t}_r$ has a basis consisting of the X_α of height $h(\alpha) \leqq r$ which satisfy the following conditions:*

$(*)_r$ *If $\alpha = (\alpha_1, \cdots, \alpha_n)$, then $\alpha_i = 0$ for $i \notin J_r$, $\alpha_i < p^{r+1-k}$ for $i \in J_k - J_{k-1}$, $0 \leqq k \leqq r$, and $\alpha_i < p^{r+1}$ for $i \in I = J_{-1}$.*

c) *The Lie algebra $\mathfrak{m}_r$ is identical to $(\mathfrak{g}_r \cap \mathfrak{N}) + (\mathfrak{g}_r \cap \mathfrak{H}) + \mathfrak{t}_{r-1}$.*

Observe that from Lemma 1 and the fact that $\mathfrak{s}_r \cap \mathfrak{N}$ (resp. $\mathfrak{t}_r$) is a subalgebra, it follows that the Z_α such that $h(\alpha) \leqq r$ and $\alpha \in N^I$ form a basis of $\mathfrak{s}_r \cap \mathfrak{N}$, and the Z_α satisfying $(*)_r$ and such that $h(\alpha) \leqq r$ a basis of $\mathfrak{t}_r$. We note also that the last remark before (B_r) means that G verifies conditions (B_0).

Let $\mathfrak{u}_{r+1}$ be the vector space consisting of the elements $X \in \mathfrak{g}_{r+1}$ such that $X^0 - 1 \otimes X - X \otimes 1 \in \mathfrak{t}_r \otimes \mathfrak{t}_r$. Let $\mathfrak{n}$ be the space having as a basis the $X_{r+1,i}$ of index $i \in I = J_{-1}$, $\mathfrak{q}_k$ the space having as a basis the $X_{r+1-k,i}$ of index $i \in J_k - J_{k-1}$ $(0 \leqq k \leqq r)$, $\mathfrak{r}$ the space having as a basis the X_{0i} for $i \notin J_r$. Then it is immediate to check that:

(i) $\mathfrak{u}_{r+1}$ *is the direct sum of* $\mathfrak{t}_r$, $\mathfrak{n}$, *the* $\mathfrak{q}_k$ $(0 \leqq k \leqq r)$ *and* $\mathfrak{r}$.

Next we show that:

(ii) *If* $X \in \mathfrak{u}_{r+1}$ *and* $T \in \mathfrak{s}_r \cap \mathfrak{N}$, *then* $[X, T] \in \mathfrak{t}_r$.

As $\mathfrak{u}_{r+1} \subset \mathfrak{g}_{r+1}$, $[X, T] \in \mathfrak{s}_r$. It is enough of course to take $T = Z_\alpha$ with $h(\alpha) \leqq r$ and $\alpha \in N^I$; we use induction on $|\alpha|$. For $|\alpha| = 1$, we have $T = X_{0i}$ with $i \in I$; by definition $X^0 = 1 \otimes X + X \otimes 1 + \sum_j U_j \otimes V_j$, with U_j, V_j in $\mathfrak{t}_r$, and on the other hand $X^0{}_{0i} = 1 \otimes X_{0i} + X_{0i} \otimes 1$; hence

$$[X, X_{0i}]^0 = [X^0, X^0{}_{0i}] = 1 \otimes [X, X_{0i}] + [X, X_{0i}] \otimes 1 \\ + \sum_j U_j \otimes [V_j, X_{0i}] + \sum_j [U_j, X_{0i}] \otimes V_j.$$

Now, as $X_{0i} \in \mathfrak{t}_r$, so are $[U_j, X_{0i}]$ and $[V_j, X_{0i}]$, hence we see that $[X, X_{0i}]$ belongs to $\mathfrak{u}_{r+1}$. But on the other hand, $[X, X_{0i}]$ belongs to the normal ideal $\mathfrak{a}$ generated by $\mathfrak{N}^+$ in $\mathfrak{G}$; but from (i) it follows at once (remembering that $\mathfrak{a}$ is also the right ideal generated by $\mathfrak{N}^+$) that $\mathfrak{s}_r \cap \mathfrak{u}_{r+1} \cap \mathfrak{a}$ is contained in $\mathfrak{t}_r$.

Next assume we have proved that $[X, Z_\lambda] \in \mathfrak{t}_r$ for $\lambda < \alpha$; then we have by definition $Z^0{}_\alpha = 1 \otimes Z_\alpha + Z_\alpha \otimes 1 + \sum_{0<\beta<\alpha} Z_\beta \otimes Z_{\alpha-\beta}$; hence

$$[X, Z_\alpha]^0 = [X^0, Z^0{}_\alpha] = 1 \otimes [X, Z_\alpha] + [X, Z_\alpha] \otimes 1 + \sum_{0<\beta<\alpha} Z_\beta \otimes [X, Z_{\alpha-\beta}] \\ + \sum_{0<\beta<\alpha} [X, Z_\beta] \otimes Z_{\alpha-\beta} + \sum_j \sum_{0 \leqq \beta \leqq \alpha} (U_j Z_\beta \otimes V_j Z_{\alpha-\beta} - Z_\beta U_j \otimes Z_{\alpha-\beta} V_j).$$

But as $[X, Z_\beta] \in \mathfrak{t}_r$ for $\beta < \alpha$ by the induction hypothesis, we first conclude as above that $[X, Z_\alpha] \in \mathfrak{u}_{r+1}$, and then that $[X, Z_\alpha] \in \mathfrak{t}_r$. Our next step consists first in defining, by the same process as in Theorem 1, for each $i \in I$, an element $Y_{r+1,i}$ belonging to $\mathfrak{g}_{r+1} \cap \mathfrak{N}$ and such that $Y_{r+1,i} = X_{r+1,i} + \sum_{j=1}^{n} a_{ij} X_{0j}$. On the other hand, for $i \in J_k - J_{k-1}$ $(0 \leqq k \leqq r)$ we can write $X_{r-k,i} = S + T + U$, with $S \in \mathfrak{g}_r \cap \mathfrak{S}$, $T \in \mathfrak{g}_r \cap \mathfrak{N}$, $U \in \mathfrak{t}_{r-1}$. Let $S' \in \mathfrak{g}_{r+1} \cap \mathfrak{S}$, $T' \in \mathfrak{g}_{r+1} \cap \mathfrak{N}$, $U' \in \mathfrak{t}_r$ be such that $\boldsymbol{p}'(S') = S$, $\boldsymbol{p}'(T') = T$, $\boldsymbol{p}'(U') = U$. By definition, $Y_{r-k+1,i} = S' + T' + U'$ is in $\mathfrak{u}_{r+1}$, and if we write that $\boldsymbol{p}'(Y_{r-k+1,i}) = X_{r-k,i}$, we see at once that we can write $Y_{r-k+1,i} = X_{r-k+1,i} + \sum_{j=1}^{n} a_{ij} X_{0j} + V$

with $V\in\mathfrak{t}_r$; we thus see that, by substracting V from U', we can find an element $Y_{r-k+1,i}$ in $(\mathfrak{g}_{r+1}\cap\mathfrak{H})+(\mathfrak{g}_{r+1}\cap\mathfrak{N})+\mathfrak{t}_r$, of the form $X_{r-k+1,i}+\sum_{j=1}^{n}a_{ij}X_{0j}$. It is clear that all the Y_{hi} thus defined are linearly independent $\bmod \mathfrak{t}_r$; if $\mathfrak{v}$ is the space having these Y_{hi} as a basis, $\mathfrak{v}$ is contained in $(\mathfrak{g}_{r+1}\cap\mathfrak{H})+(\mathfrak{g}_{r+1}\cap\mathfrak{N})+\mathfrak{t}_r$, and $\mathfrak{u}_{r+1}$ is the direct sum $\mathfrak{t}_r+\mathfrak{v}+\mathfrak{r}$; therefore we can find a certain number of elements $Y_{0i}\in\mathfrak{r}$ $(1\leqq i\leqq q)$ which form a basis of a supplementary subspace of $\mathfrak{v}+\mathfrak{t}_r$ in $(\mathfrak{g}_{r+1}\cap\mathfrak{N})+(\mathfrak{g}_{r+1}\cap\mathfrak{H})+\mathfrak{t}_r$.

(iii) *If* $T\in\mathfrak{g}_{r+1}\cap\mathfrak{N}$ *and* $U\in\mathfrak{t}_r$, *then* $[T,U]\in\mathfrak{t}_r$.

This is trivial if $T\in\mathfrak{s}_r\cap\mathfrak{N}\subset\mathfrak{t}_r$, and we can thus only consider the case $T=Y_{r+1,i}$, $i\in I$. As $Y_{r+1,i}\in\mathfrak{u}_{r+1}$, $Y^0_{r+1,i}-1\otimes Y_{r+1,i}-Y_{r+1,i}\otimes 1$ belongs to $\mathfrak{t}_r\otimes\mathfrak{t}_r$. We can on the other hand take $U=Z_\alpha$ with α satisfying $(^*)_r$, and then prove (iii) by induction on $|\alpha|$; the proof follows exactly the same lines as that of (ii), and we omit it.

(iv) *If* $T\in\mathfrak{g}_{r+1}\cap\mathfrak{N}$, $U\in\mathfrak{u}_{r+1}$, *then* $[T,U]\in(\mathfrak{g}_{r+1}\cap\mathfrak{N})+\mathfrak{t}_r$.

Due to (ii), we can suppose $T=Y_{r+1,i}$, $i\in I$; then the proof again follows the same lines as (ii), using the fact that $Y^0_{r+1,i}-1\otimes Y_{r+1,i}-Y_{r+1,i}\otimes 1$ is in $(\mathfrak{s}_r\cap\mathfrak{N})\otimes(\mathfrak{s}_r\cap\mathfrak{N})$, the results (ii) and (iii), and noting that $\mathfrak{u}_{r+1}\cap\mathfrak{a}\subset(\mathfrak{g}_{r+1}\cap\mathfrak{N})+\mathfrak{t}_r$.

(v) *The Lie-p-algebra* $\mathfrak{m}_{r+1}$ *is identical to* $(\mathfrak{g}_{r+1}\cap\mathfrak{N})+(\mathfrak{g}_{r+1}\cap\mathfrak{H})+\mathfrak{t}_r$.

By definition of $\mathfrak{m}_r$, it is enough to prove that $\mathfrak{m}'_{r+1}=(\mathfrak{g}_{r+1}\cap\mathfrak{N})+(\mathfrak{g}_{r+1}\cap\mathfrak{H})+\mathfrak{t}_r$ is a Lie-p-algebra. For any two elements X,X' of $\mathfrak{m}'_{r+1}$, we have $X+T+U\in\mathfrak{g}_{r+1}\cap\mathfrak{H}$, $X'+T'+U'\in\mathfrak{g}_{r+1}\cap\mathfrak{H}$ for suitable elements T,T' in $\mathfrak{g}_{r+1}\cap\mathfrak{N}$, U,U' in $\mathfrak{t}_r$. As $[X+T+U,X'+T'+U']$ is in $\mathfrak{g}_{r+1}\cap\mathfrak{H}$, X,X' in $\mathfrak{u}_{r+1}$, it follows from (ii) and (iv) that $[X,X']$ belongs to $\mathfrak{m}'_{r+1}$. Similarly $(X+T+U)^p\in\mathfrak{g}_{r-1}\cap\mathfrak{H}$; but by Jacobson's formula, $(X+T+U)^p$ is the sum of $X^p+T^p+U^p$ and of alternants formed with X, T and U; we have just seen that the latter are in $\mathfrak{m}'_{r+1}$, and as $U^p\in\mathfrak{t}_r$ and $T^p\in\mathfrak{g}_{r+1}\cap\mathfrak{N}$, we have again $X^p\in\mathfrak{m}'_{r+1}$, which concludes the proof of (v).

This shows that q is the number of elements of $J_{r+1}-J_r$, and that the Y_{0i} are linear combinations of the X_{0j} of index $j\in J_{r+1}-J_r$, let $Y_{0i}=\sum_{j\in J_{r+1}-J_r}b_{ij}X_{0j}$; let (c_{ij}) be the inverse matrix to (b_{ij}). Consider the isomorphism u of G onto a group G' defined by

$$u_i(x)=h_i(x)-\sum_{k=-1}^{r}\Big(\sum_{j\in J_k-J_{k-1}}a_{ji}x_j^{p^{r-k+1}}\Big)\qquad\text{(taking } J_{-2}=\emptyset)$$

where $h_i(\mathbf{x}) = x_i$ if $i \notin J_{r+1} - J_r$, and $h_i(\mathbf{x}) = \sum_{j \in J_{r+1} - J_r} c_{ji} x_j$ if $i \in J_{r+1} - J_r$. Then it follows readily from the definitions [9, p. 221] that

$$
\begin{aligned}
&\mathbf{u}'(Z_\alpha) = Z'_\alpha \text{ for indices } \alpha \text{ verifying } (*)_r \\
(12) \qquad &\mathbf{u}'(Y_{r-k+1,i}) = X'_{r-k+1,i} \text{ for } i \in J_k - J_{k-1}, \qquad -1 \leqq k \leqq r+1 \\
&\mathbf{u}'(X_{0i}) = X'_{0i} \text{ for } i \notin J_{r+1} - J_r.
\end{aligned}
$$

The group law of G' is now not pseudo-canonical any more, and we have to apply to G' the isomorphism $\mathbf{v}$ onto a group G'' obtained by the "standard process" of no. 3. Now, if $\mathbf{f}$ is the homomorphism of $\mathfrak{H}_n(K)$ onto $\mathfrak{G}$ such that $\mathbf{f}(V_\alpha) = Z_\alpha$ for every index α, it follows from (12) that $\mathbf{u}'(\mathbf{f}(V_\alpha)) = Z'_\alpha$ for all α verifying $(*)_r$. As explained in no. 3, $\mathbf{v}$ is obtained as an "infinite product" $\cdots \mathbf{v}_h \mathbf{v}_{h-1} \cdots \mathbf{v}_0$; using the preceding remark and the recursive definition of the $\mathbf{v}_h$, it is easily verified by induction that for any h, $\mathbf{v}'_h(Z^{(h)}_\alpha) = Z^{(h+1)}_\alpha$ for all α satisfying $(*)_r$ and in addition

$$\mathbf{v}'_h(X^{(h)}_{r-k+1,i}) = X^{(h+1)}_{r-k+1,i} \text{ for } i \in J_k - J_{k-1}, \qquad -1 \leqq k \leqq r+1,$$

as well as $\mathbf{v}'_h(X^{(h)}_{0i}) = X^{(h+1)}_{0i}$ for $1 \leqq i \leqq n$ (with self-explanatory notations). We suppress the somewhat tedious detail, which involves not the slightest difficulty, the main point being the following one: if, in an arbitrary power series without constant term, we substitute for the indeterminates power series in the x_i $(1 \leqq i \leqq n)$, in which there is no monomial in $\mathbf{x}^\alpha$ with α satisfying $(*)_r$, or $\alpha = p^{r-k+1}\epsilon_i$, $i \in J_k - J_{k-1}$ $(-1 \leqq k \leqq r+1)$, or $\alpha = \epsilon_i$ $(1 \leqq i \leqq n)$ then there is also no monomial of any of these types in the power series which results from the substitution. The same remark shows that if we consider the isomorphism $\mathbf{w} = \mathbf{v} \circ \mathbf{u}$ of G onto G'', there are no monomials in $\mathbf{x}^\alpha$ with α satisfying $(*)_r$ in any of the series $w_i(\mathbf{x}) - x_i$.

Replacing for a moment G by G'', we have obtained as a basis for $\mathfrak{m}_{r+1}$ the X_α which satisfy $(*)_r$ and the $X_{r-k+1,i}$ such that $i \in J_k - J_{k-1}$ $(-1 \leqq k \leqq r+1)$. As $\mathfrak{m}_{r+1}$ is a Lie-p-algebra, it is immediate to see that the associative algebra $\mathfrak{t}_{r+1}$ it generates has as a basis the X_α which satisfy $(*)_{r+1}$. In other words, we have obtained a group for which (B_{r+1}) holds.

Summing up what we have done, and changing the notations, we have proved the following result: if G_r is a group, H_r a subgroup and N_r a normal subgroup of G_r for which assumptions (B_r) are satisfied, then there is an isomorphism $\mathbf{g}_r$ of G_r onto a group G_{r+1} such that $H_{r+1} = \mathbf{g}_r(H_r)$ and $N_{r+1} = \mathbf{g}_r(N_r)$ now satisfy assumptions (B_{r+1}). Moreover, as soon as $r > t$, in the power series $g_{ri}(\mathbf{x}) - x_i$ $(1 \leqq i \leqq n)$ there are no monomials of height $< r - t$. We conclude as usual (see end of proof of Theorem 1), obtaining an isomorphism $\boldsymbol{g}$ of G onto a group $\bar{G}$ such that if $\bar{H}=\boldsymbol{g}(H)$ and $\bar{N}=\boldsymbol{g}(N)$ $\bar{H}$ and $\bar{N}$ now satisfy assumptions (B_r) for *every* r. The subalgebra of $\bar{\mathfrak{G}}$ generated by $\bar{\mathfrak{H}} \cup \bar{\mathfrak{N}}$ is then the algebra having as a basis the $\bar{Z}_\alpha$ such that $\alpha \in \mathbf{N}^{J_1}$, and it is clear that it is a typical subhyperalgebra; the proof of Theorem 3 is thus complete.

From Corollary 2 to Proposition 9 and the chain conditions, it follows that the normal subgroups of G form a *complete lattice*. There is a corresponding result for the normal ideals of $\mathfrak{G}$:

PROPOSITION 10. *The normal ideals of* $\mathfrak{G}$ *form a complete lattice; more precisely, the mapping* $\mathfrak{N} \rightarrow \mathfrak{a}(\mathfrak{N})$ *which, to every subhyperalgebra* $\mathfrak{N}$ *corresponding to a normal subgroup of* G, *associates the normal ideal it generates, is a lattice isomorphism, such that* $\mathfrak{a}(\mathfrak{N}_1 \vee \mathfrak{N}_2)=\mathfrak{a}(\mathfrak{N}_1)+\mathfrak{a}(\mathfrak{N}_2)$.

Indeed, by Theorem 3, $\mathfrak{a}(\mathfrak{N}_1)+\mathfrak{a}(\mathfrak{N}_2)$ is the ideal generated by the subalgebra of $\mathfrak{G}$ generated by $\mathfrak{N}_1 \cup \mathfrak{N}_2$, hence by $\mathfrak{N}_1 \vee \mathfrak{N}_2$. It is clear that the condition $\mathfrak{N}_1 \subset \mathfrak{N}_2$ implies $\mathfrak{a}(\mathfrak{N}_1) \subset \mathfrak{a}(\mathfrak{N}_2)$; conversely, if that last inclusion holds, then $\mathfrak{a}(\mathfrak{N}_1 \vee \mathfrak{N}_2)=\mathfrak{a}(\mathfrak{N}_2)$. If we had $\mathfrak{N}_1 \vee \mathfrak{N}_2 \neq \mathfrak{N}_2$, the dimension of $N_1 \vee N_2$ would be strictly greater than that of N_2; but the dimension of a normal subgroup N is equal to $\dim(\mathfrak{g}_c \cap \mathfrak{a}(\mathfrak{N}))$, hence our conclusion.

10. The isomorphism theorems and the Jordan-Hölder theorem.

For convenience, we collect the properties corresponding to the classical "isomorphism theorems" of ordinary group theory:

PROPOSITION 11. *Let* $\boldsymbol{u}$ *be a homomorphism of* G *onto a group* G', *having kernel* $N=\boldsymbol{u}^{-1}(e)$. *Then:*

a) *The mapping* $H \rightarrow \boldsymbol{u}(H)$ *is a bijection of the set of subgroups of* G *containing* N, *onto the set of subgroups of* G', *the inverse bijection being* $H' \rightarrow \boldsymbol{u}^{-1}(H')$.

b) *In the preceding one-to-one correspondence, to normal subgroups correspond normal subgroups, and the correspondence is a lattice isomorphism. Moreover, if* $H \supset N$ *is normal in* G, *and* $H'=\boldsymbol{u}(H)$, *there is an isogeny of* G/H *onto* G'/H', *and both groups are isomorphic when* $\boldsymbol{u}$ *is an epimorphism.*

c) *If* F *is an arbitrary subgroup of* G, $F \vee N=\boldsymbol{u}^{-1}(\boldsymbol{u}(F))$, *there exist isogenies of* $F/(F \wedge N)$ *onto* $(F \vee N)/N$ *and of* $(F \vee N)/N$ *onto* $\boldsymbol{u}(F)$. *Moreover,* $\dim F+\dim N=\dim(F \vee N)+\dim(F \wedge N)$.

Most of this has already been proved (Propositions 8 and 9). The fact that if H is normal in G, $\boldsymbol{u}(H)$ is normal in G' follows from the characterization of the subhyperalgebras of normal subgroups given in Theorem 2, remembering that $\boldsymbol{u}'(\mathfrak{G})=\mathfrak{G}'$. Conversely, if H' is normal in G', and $\boldsymbol{v}$ is the natural epimorphism of G' onto G'/H', $\boldsymbol{v}\circ\boldsymbol{u}$ is a homomorphism of G onto G'/H', of kernel $H=\boldsymbol{u}^{-1}(H')$, hence H is normal in G and there is an isogeny of G/H onto G'/H' (Proposition 6); this isogeny is an isomorphism when $\boldsymbol{u}$ is an epimorphism, since then $\boldsymbol{v}\circ\boldsymbol{u}$ is an epimorphism (Corollary to Proposition 1). The isogenies of $(F\vee N)/N$ and $F/(F\wedge N)$ onto $\boldsymbol{u}(F)$ stem from application of Proposition 6 to the restrictions of $\boldsymbol{u}$ to $F\vee N$ and F respectively. If we replace $\boldsymbol{u}$ by the natural epimorphism of G onto G/N, it follows from Proposition 1 that the restriction of $\boldsymbol{u}$ to $F\vee N$ is an epimorphism onto $\boldsymbol{u}(F)$; in that case $\boldsymbol{u}(F)$ and $(F\vee N)/N$ are isomorphic, hence the existence of an isogeny of $F/(F\wedge N)$ onto $(F\vee N)/N$ (cf. no. 21).

COROLLARY. *Under the same assumptions as in Proposition* 11, *the mapping* $\mathfrak{a}(\mathfrak{H})\rightarrow\boldsymbol{u}'(\mathfrak{a}(\mathfrak{H}))$ *is a lattice isomorphism of the set of normal ideals* $\mathfrak{a}(\mathfrak{H})$ *corresponding to normal subgroups* H *of* G *containing* N, *onto the set of all normal ideals of* $\mathfrak{G}'$, *the inverse mapping being* $\mathfrak{a}(\mathfrak{H}')\rightarrow\boldsymbol{u}'^{-1}(\mathfrak{a}(\mathfrak{H}'))$.

It is now possible to develop the sequence of propositions and definitions corresponding to the one which, for abstract groups (or Lie groups over fields of characteristic 0), leads to the *Jordan-Hölder theorem*: namely the Zassenhaus lemma, the definition of simple groups[7a] and the Schreier refinement th[illegible]. The only difference is that throughout "*isomorphic groups*" ar[illegible] *isogenous groups*"; "equivalent" composition series a[illegible]uotient groups can be paired so as to be *isogenous*; [illegible]heorem states then that two Jordan-Hölder series [illegible]ss the details, which are straightforward adapta- [illegible]see e.g. [3, pp. 84-87], and [16, pp. 422-423], [illegible]for algebraic groups); as we have not yet [illegible]groups, the only point where a little care [illegible]f the g.l.b. $G_i\wedge H_j$ when $(G_i)_{0\leqq i\leqq n}$ [illegible] of G. This is done for instance [illegible]rmal in H_j, hence that $(G_i\wedge H_j)$ [illegible]ld be observed that this is the

11. Commuting subgroups and center. Let (H, f) and (H', g) be two subgroups of G; we say they *commute* ("elementwise" [8]) or that they *centralize* each other if $f(y)g(y') = g(y')f(y)$ for any independent generic points y, y' of H, H' respectively.

Proposition 12. *In order that two subgroups of G commute, it is necessary and sufficient that their subhyperalgebras commute elementwise in $\mathfrak{G}$.*

Let (Y_λ), (Y'_μ) and (Z_α) be the structural bases of $\mathfrak{H}$, $\mathfrak{H}'$, $\mathfrak{G}$ respectively. If we put $(f(y))^\alpha = \sum_\lambda a_{\lambda\alpha} y^\lambda$, $(g(y'))^\beta = \sum_\mu b_{\mu\beta} y'^\mu$, the relation $f(y)g(y') = g(y')f(y)$ is by definition equivalent to the relations

$$\sum_{\alpha,\beta,\lambda,\mu} d_{\alpha\beta\gamma} a_{\lambda\alpha} b_{\mu\beta} y^\lambda y'^\mu = \sum_{\alpha,\beta,\lambda,\mu} d_{\alpha\beta\gamma} b_{\mu\alpha} a_{\lambda\beta} y^\lambda y'^\mu$$

for any index γ. This yields $\sum_{\alpha,\beta} d_{\alpha\beta\gamma} a_{\lambda\alpha} b_{\mu\beta} = \sum_{\alpha,\beta} d_{\alpha\beta\gamma} b_{\mu\alpha} a_{\lambda\beta}$ for all λ, μ. But we have $f'(Y_\lambda) = \sum_\alpha a_{\lambda\alpha} Z_\alpha$ and $g'(Y'_\mu) = \sum_\alpha b_{\mu\alpha} Z_\alpha$, hence the preceding relations are equivalent to $f'(Y_\lambda) g'(Y'_\mu) = g'(Y'_\mu) f'(Y_\lambda)$, q. e. d.

Proposition 12 and Theorem 2 show immediately that any subgroup of G which centralizes G is a *normal* subgroup of G; if Z_1, Z_2 are any such subgroups, $Z_1 \vee Z_2$ is therefore defined and a normal subgroup of G; and it follows from Proposition 12 and Theorem 3 that $Z_1 \vee Z_2$ again centralizes G. There is therefore a *largest* subgroup centralizing G, the *center* Z (or $Z(G)$) of G, which is an abelian normal subgroup. It follows [illegible] Proposition 12 that the subhyperalgebra $\mathfrak{Z}$ of the center Z [illegible]*peralgebra contained in the center* of the algebra $\mathfrak{G}$. [illegible]

12. Quasi-direct products. We say that a g[illegible] *product* of two of its subgroups H_1, H_2, if th[illegible] direct product $G_1 \times G_2$ onto G such that $u($[illegible]

Proposition 13. *In order that a*[illegible] *two subgroups H_1, H_2, necessary an*[illegible] *H_2 be normal subgroups such tha*[illegible] *these conditions are satisfied, H_1*[illegible]

A group G will be called *solvable* (resp. *nilpotent*) if $D^n(G)=e$ (resp. $C^n(G)=e$) for sufficiently large n. From Propositions 16 and 17 it follows that subgroups and quotient groups of solvable (resp. nilpotent) groups are solvable (resp. nilpotent). The usual arguments show that solvable groups are characterized as those having a composition series with abelian quotient groups, and that if H is solvable and normal in G, and G/H solvable, then G is solvable.

The *ascending central series* is also defined as usual: $Z^1(G)$ is the center of G and $Z^n(G)$ the inverse image of the center of $G/Z^{n-1}(G)$. As, by definition, $C^{n-1}(G)/C^n(G)$ is contained in the center of $G/C^n(G)$, the classical argument shows that nilpotent groups are also those for which the ascending central series terminates at G.

III. Representable Groups.

14. Formal Lie groups **associated to algebraic groups.**[10] The words "algebraic group" will be taken with the meaning given to them in [16]. The process outlined in [8, p. 116], associating a formal Lie group to an algebraic group which is an affine variety, can be generalized in an obvious way to arbitrary algebraic groups. We rapidly sketch it in this section.

We first recall known properties of *local rings* at simple points of algebraic varieties. Let U, V be two algebraic varieties, F an everywhere defined rational map of U into V, K a common field of definition of U, V, F, a a simple point of U rational over K, b a simple point of V rational over K, and suppose $b=F(a)$. Let x, y be generic points of U, V over K, and consider an element $t(y)\in K(y)$ of the local ring $\mathfrak{o}_K(b,V)$ of V at the point b. As the specialization $y\to b$ transforms $t(y)$ into a finite element $t(b)$ and the specialization $x\to a$ transforms $F(x)$ into b, the specialization $y\to F(x)$ transforms $t(y)$ into a finite $t(F(x))$, which is an element of the local ring $\mathfrak{o}_K(a,U)$, and the mapping $t(y)\to t(F(x))$ is a homomorphism of $\mathfrak{o}_K(b,V)$ into $\mathfrak{o}_K(a,U)$, which can be extended by continuity to a homomorphism $\bar{F}$ of the completed local ring $\mathfrak{O}_K(b,V)$ into the completed local ring $\mathfrak{O}_K(a,U)$. If $\dim U=m$, $\dim V=n$, then $\mathfrak{O}_K(a,U)$ (resp. $\mathfrak{O}_K(b,V)$) can be identified to the ring of power series $K[[X_1,\cdots,X_m]]$ (resp.

---

[10] The assumption that the characteristic is $\neq 0$ is not used in this part until no. 19 (Lemma 3 and its consequences). Taking into account the one-to-one correspondence between formal Lie groups and Lie algebras in characteristic 0, the theorems proved in nos. 14-18 yield new proofs of the corresponding theorems on Lie algebras proved by Chevalley in [6].

$K[[Y_1,\cdots,Y_n]]$) in m (resp. n) indeterminates, by an isomorphism which sends a system $(s_i)_{1\leq i\leq m}$ (resp. $(t_j)_{1\leq j\leq n}$) of uniformizing parameters in $\mathfrak{o}_K(a,U)$ (resp. $\mathfrak{o}_K(b,V)$) onto the system (X_i) (resp. (Y_j)); the elements $\bar{F}(t_j)$ of $\mathfrak{O}_K(a,U)$ are then identified to n power series $\phi_j(X_1,\cdots,X_m)$; if t is an element of $\mathfrak{O}_K(b,V)$, identified to a power series $f(Y_1,\cdots,Y_n)$, $\bar{F}(t)$ is identified to the power series obtained by replacing each Y_j by $\phi_j(X_1,\cdots,X_m)$ in the power series $f(Y_1,\cdots,Y_n)$.

If W is a third algebraic variety, G an everywhere defined rational map of V into W, W and G being defined over K, c a simple point of W, rational over K, such that $G(b)=c$, then it is readily verified that $\overline{G\circ F}=\bar{F}\circ\bar{G}$.

In particular, suppose F is *generically surjective*, i.e. that $F(x)$ is a generic point of V over K [16]; then it is obvious that the restriction of $\bar{F}$ to $\mathfrak{o}_K(b,V)$ is injective, and it can be proved [17, p. 64, th. 3] that $\bar{F}$ itself is *injective.*

Consider now the product $U\times V$, in which (a,b) is a simple point; to the projections pr_U and pr_V correspond natural injections of $\mathfrak{o}_K(a,U)$ and $\mathfrak{o}_K(b,V)$ into $\mathfrak{o}_K((a,b),U\times V)$; the images $s'_1,\cdots,s'_m,t'_1,\cdots,t'_n$ of the s_i and t_j by these injections form a system of $m+n$ uniformizing parameters of $U\times V$ at the point (a,b), which we will say *corresponds naturally* to the systems (s_i) and (t_j).

Finally, suppose U is a subvariety of V, $b=a$, F being the natural injection of U into V. Then $\bar{F}$ is a homomorphism of $\mathfrak{O}_K(a,V)$ *onto* $\mathfrak{O}_K(a,U)$; and it can be shown that uniformizing parameters t_i in $\mathfrak{o}_K(a,V)$ may be chosen so that the kernel of $\bar{F}$ is the ideal generated by $t_{m+1},\cdots,t_n$, and the $\bar{F}(t_i)$ for $1\leqq i\leqq m$ form a system of uniformizing parameters of $\mathfrak{o}_K(a,U)$ [4, p. 705, prop. 9].

Let now G be an algebraic group of dimension n defined over K, G_0 the connected component of the identity e in G. Applying the process described above to the rational mapping $f\colon (x,y)\to xy$ of $G_0\times G_0$ into G_0, we obtain a homomorphism $\bar{f}$ of $\mathfrak{O}_K(e,G_0)$ into $\mathfrak{O}_K((e,e),G_0\times G_0)$; let $(t_i)_{1\leq i\leq n}$ be a system of uniformizing parameters in $\mathfrak{o}_K(e,G_0)$, and let $(t'_1,\cdots,t'_n,t''_1,\cdots,t''_n)$ be the system of uniformizing parameters corresponding naturally to (t_i) in $\mathfrak{o}_K((e,e),G_0\times G_0)$; then, if (t'_i) and (t''_i) are identified to two systems $\mathbf{x}=(x_i)$, $\mathbf{y}=(y_i)$ of n indeterminates, each element $\bar{f}(t_i)$ is identified to a power series $\phi_i(\mathbf{x},\mathbf{y})$ in these $2n$ indeterminates. Consideration of the composed mappings $(x,y,z)\to(xy,z)\to xyz$, $(x,y,z)\to(x,yz)\to xyz$ of $G_0\times G_0\times G_0$ into G_0, and of the composed mappings $x\to(x,e)\to xe$, $x\to(e,x)\to ex$ of G_0 into itself proves at once that the power series ϕ_i define a *group law* over K. Let us for the moment denote by $G^*((t_i))$ the formal Lie group thus associated to G, K and (t_i); it is immediate that when K is replaced by a larger field of definition L of G, the power series ϕ_i are not changed, in other words $G^*((t_i))$ is replaced by $(G^*((t_i)))_{(L)}$.

Let now H be a second algebraic group of dimension m, e' the identity in H, H_0 its connected component, u a rational homomorphism of G into H, K a field of definition for G, H and u[11]; it is known that u, restricted to G_0, is a rational homomorphism of G_0 into the connected component H_0 of H. It gives rise therefore to a homomorphism $\bar{u}$ of $\mathfrak{O}_K(e', H_0)$ into $\mathfrak{O}_K(e, G_0)$. Let $(s_j)_{1\leq j\leq m}$ be a system of uniformizing parameters in $\mathfrak{o}_K(e', H_0)$; then, if (t_i) is identified to a system $\boldsymbol{x}=(x_i)$ of n indeterminates, each element $\bar{u}(s_j)$ is identified to a power series $u_j(\boldsymbol{x})$ in these n indeterminates; and consideration of the composed mappings $(x,y)\rightarrow(u(x),u(y))\rightarrow u(x)u(y)$ and $(x,y)\rightarrow xy\rightarrow u(xy)$ of $G_0\times G_0$ into H_0 shows that the system $\boldsymbol{u}=(u_j)$ of m power series is a *homomorphism* of $G^*((t_i))$ into $H^*((s_j))$. If u is a rational homomorphism of G into G', v a rational homomorphism of G' into G'', then (with self-explanatory notations) if we consider the rational homomorphism $w=v\circ u$ of G into G'', the corresponding homomorphisms $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$ of $G^*((t_i))$ into $G'^*((t'_j))$, of $G'^*((t'_j))$ into $G''^*((t''_k))$ and of $G^*((t_i))$ into $G''^*((t''_k))$ are such that $\boldsymbol{w}=\boldsymbol{v}\circ\boldsymbol{u}$. If we take in particular $G=G'=G''$, u, v being the identity, and $t''_i=t_i$, we see that the various formal Lie groups $G^*((t_i))$ corresponding to different systems of uniformizing parameters, are isomorphic. We will therefore usually write from now on G^* to denote one of these groups.

Suppose H is a closed subgroup of dimension $m<n$ of the algebraic group G, and take a system (t_i) of uniformizing parameters of $\mathfrak{o}_K(e, G_0)$ such that, if u is the natural injection of H into G, the kernel of $\bar{u}$ is generated by the t_i of index $>m$, and the elements $\bar{u}(t_i)$ for $i\leq m$ form a system of uniformizing parameters of $\mathfrak{o}_K(e, H_0)$. With that choice of uniformizing parameters, it is clear that the formal Lie group H^* will be the typical subgroup of G^* defined by the equations $x_i=0$ for $i>m$.

PROPOSITION 18. *If u is a rational homomorphism of an algebraic group G into an algebraic group H, having kernel N, then, if $\boldsymbol{u}$ is the*

---

[11] From now on, we will assume (unless the contrary is explicitly stated) that whenever the field K is mentioned in connection with algebraic groups or rational homomorphisms, it is a common field of definition of all points, algebraic groups and rational homomorphisms concerned. We recall that no fields other than *perfect* fields are ever considered in this paper, which suppresses the distinction between field of definition and "field of quasi-definition" [2, p. 25].

corresponding homomorphism[12] *of* G^* *into* H^*, N^* *is the kernel of* $\mathbf{u}$, $\mathbf{u}(G^*) = (u(G))^*$ *and the rank of* $\mathbf{u}$ *is equal to the rank of* u.

Let K be a common field of definition of G, H and u. As u can be considered as composed of the natural injection of $u(G)$ into H and of a surjective homomorphism defined over K [16, p. 415, cor. 1 to th. 4], we can immediately restrict ourselves to the case in which u is *surjective.* If v is the natural injection of N into G, $\mathbf{v}$ the corresponding monomorphism of N^* into G^*, then from $u(v(N)) = \{e'\}$ follows $\mathbf{u}(\mathbf{v}(N^*)) = \mathbf{e}'$, in other words N^* is contained in the kernel N' of $\mathbf{u}$. Suppose $N' \neq N^*$; then, if $\dim G = n$, $\dim H = m$, we would have $\dim N' > n - m$ [2, prop. 5.2, p. 37]; by a change of variables, we may suppose N' is a typical subgroup of G^*, and then the definition of $\mathbf{u}$ shows that the image of $\mathfrak{O}_K(e', H_0)$ by $\bar{u}$ would be a ring of power series in less than m indeterminates; but this contradicts the fact that $\bar{u}$ is an *isomorphism* of $\mathfrak{O}_K(e', H_0)$ onto its image in $\mathfrak{O}_K(e, G_0)$. Then the dimensions of $\mathbf{u}(G^*)$ and $(u(G))^*$ are equal, and this ends the proof.

This result implies immediately that, for any algebraic subgroup F of G, $\mathbf{u}(F^*) = (u(F))^*$, and, for any algebraic subgroup $F' \subset u(G)$, $\mathbf{u}^{-1}(F'^*) = (u^{-1}(F'))^*$,[13] the latter relation being again due to the fact that the dimensions of both groups are the same, and that the first contains the second by definition.

If H_1, H_2 are two algebraic subgroups of G which *commute* (elementwise), it is immediately verified that H^*_1 and H^*_2 commute in G^*.

PROPOSITION 19. *If* N_1, N_2 *are two connected normal algebraic subgroups of* G, *then* $[N_1, N_2]^* = [N^*_1, N^*_2]$.

If u is the natural homomorphism of G onto $G/[N_1, N_2]$, $u(N_1)$ and $u(N_2)$ commute, hence $\mathbf{u}(N^*_1)$ and $\mathbf{u}(N^*_2)$ commute in $\mathbf{u}(G^*)$; as $[N_1, N_2]^*$ is the kernel of $\mathbf{u}$, we have $[N^*_1, N^*_2] \subset [N_1, N_2]^*$ by definition (no. 13). Let $\dim[N^*_1, N^*_2] = m$, $\dim[N_1, N_2] = q$. We can suppose the uniformizing parameters t_i $(1 \leqq i \leqq n)$ of $\mathfrak{o}_K(e, G_0)$ have been taken so that, if v is the natural injection of $[N_1, N_2]$ into G, the $s_i = \bar{v}(t_i)$ $(1 \leqq i \leqq q)$, constitute a system of uniformizing parameters of $\mathfrak{o}_K(e, [N_1, N_2]_0)$. We identify the t_i $(1 \leqq i \leqq n)$ with a system $x = (x_1, \cdots, x_n)$ of n indeterminates, the s_i

---

[12] I will systematically use the convention by which a boldface letter represents the homomorphism of formal Lie groups corresponding to a rational homomorphism of algebraic groups, denoted by the corresponding italic letter.

[13] If U is the graph of u, which is an algebraic subgroup of $G \times G'$, $u^{-1}(F')$ is the projection on G of the subgroup $U \cap (G \times F')$ of $G \times G'$.

$(1 \leqq i \leqq q)$ with a system $\boldsymbol{y} = (y_1, \cdots, y_q)$ of q indeterminates. We know it is possible to "change variables" in G^* so as to transform $[N^*_1, N^*_2]$ into a typical subgroup: this means there is a system of n power series $x'_i = \psi_i(x_1, \cdots, x_n)$ with non vanishing jacobian such that $[N^*_1, N^*_2]$ is defined by the relations $x'_i = 0$ for $m+1 \leqq i \leqq n$.

Consider now r generic points n'_j (resp. n''_j) of N_1 (resp. N_2) over K, all these points being independent; let f (resp. g) be the natural injection of N_1 (resp. N_2) into G, and consider the rational map F of $N^r_1 \times N^r_2$ into G, defined by

$$F((n'_j), (n''_j)) = (f(n'_1))(g(n''_1))(f(n'_1))^{-1}(g(n''_1))^{-1} \cdots$$
$$(f(n'_r))(g(n''_r))(f(n'_r))^{-1}(g(n''_r))^{-1};$$

by definition, one can write $F = v \circ F_1$, where F_1 is a rational map of $N^r_1 \times N^r_2$ into $[N_1, N_2]$. Take in $\mathfrak{o}_K(e, (N_1)_0)$ (resp. $\mathfrak{o}_K(e, (N_2)_0)$) a system $(w'_1, \cdots, w'_{d_1})$ (resp. $(w''_1, \cdots, w''_{d_2})$) of uniformizing parameters, and in $\mathfrak{o}_K((e, \cdots, e), (N^r_1 \times N^r_2)_0)$ the system of uniformizing parameters

$$w'_{11}, \cdots, w'_{1d_1}, w'_{21}, \cdots, w'_{2d_1}, \cdots, w'_{r1}, \cdots, w'_{rd_1},$$
$$w''_{11}, \cdots, w''_{1d_2}, \cdots, w''_{r1}, \cdots, w''_{rd_2}$$

which corresponds naturally to the w'_h and w''_h. If we identify these parameters with $2r$ systems $\mathbf{z}'_j = (z'_{jh})_{1 \leqq h \leqq d_1}$, $\mathbf{z}''_j = (z''_{jk})_{1 \leqq k \leqq d_2}$ of indeterminates $(1 \leqq j \leqq r)$, then $\bar{F}(t_i) = 0$ for $q+1 \leqq i \leqq n$, and $\bar{F}(t_i) = \bar{F}_1(s_i)$ for $1 \leqq i \leqq q$ is a power series $w_i((\mathbf{z}'_j), (\mathbf{z}''_j))$ in the z'_{jh} and z''_{jk}. But it follows from the definitions that this system of n power series is the one which we have agreed to denote by

$$f(\mathbf{z}'_1)g(\mathbf{z}''_1)f(\mathbf{z}'_1)^{-1}g(\mathbf{z}''_1)^{-1} \cdots f(\mathbf{z}'_r)g(\mathbf{z}''_r)f(\mathbf{z}'_r)^{-1}g(\mathbf{z}''_r)^{-1}$$

and from the definition of $[N^*_1, N^*_2]$ (no. 13) it follows that we have

$$(13) \qquad \psi_i(w_1((\mathbf{z}'_j), (\mathbf{z}''_j)), \cdots, w_q((\mathbf{z}'_j), (\mathbf{z}''_j)), 0, \cdots, 0) = 0$$
$$\text{for } m+1 \leqq i \leqq n.$$

Now it is known [2, pp. 34-35] that for r large enough, $F_1((n'_j), (n''_j))$ is a *generic point* of $[N_1, N_2]$. But then $\bar{F}_1$ is an *isomorphism* of $\mathfrak{O}_K(e, [N_1, N_2]_0)$ onto its image; and for $m+1 \leqq i \leqq n$, the left hand side of (13) is the image by $\bar{F}_1$ of the element of $\mathfrak{O}_K(e, [N_1, N_2]_0)$ identified to the power series $\psi_i(y_1, \cdots, y_q, 0, \cdots, 0)$. Therefore we have $\psi_i(y_1, \cdots, y_q, 0, \cdots, 0) = 0$ for $m+1 \leqq i \leqq n$; but by definition, this means that $v([N_1, N_2]^*) \subset [N^*_1, N^*_2]$, q.e.d.

COROLLARY. *In order that a connected algebraic group G be solvable (resp. nilpotent, commutative), it is necessary and sufficient that G^* be solvable (resp. nilpotent, commutative).*

15. Representable groups. By *general linear group* $GL(n)$, we will always mean the algebraic group consisting of all $n \times n$ invertible matrices with elements in the "universal domain" Ω; it is connected and defined over the prime field F_p. If (t_{ij}) are the elements of a generic matrix $T \in GL(n)$ over F_p, then we can take the $t_{ij} - \delta_{ij}$ as uniformizing parameters of $\mathfrak{o}_{F_p}(e, GL(n))$, which we call the *coordinates* of T. The corresponding formal Lie group over F_p will be denoted $GL^*(n)$; its group law is defined by the power series $\phi_{ij}(\boldsymbol{x}, \boldsymbol{y})$ (with $\boldsymbol{x} = (x_{ij})$, $\boldsymbol{y} = (y_{ij})$, $1 \leqq i, j \leqq n$)

$$\delta_{ij} + \phi_{ij}(\boldsymbol{x}, \boldsymbol{y}) = \sum_{k=1}^{n} (\delta_{ik} + x_{ik})(\delta_{kj} + y_{kj}). \tag{14}$$

A homomorphism $\boldsymbol{u}$ of a formal Lie group G (over a field K) into $GL^*(n)$ is therefore a system (u_{ij}) of n^2 power series (with coefficients in K) verifying the identities

$$\delta_{ij} + u_{ij}(\boldsymbol{x}\boldsymbol{y}) = \sum_{k=1}^{n} (\delta_{ik} + u_{ik}(\boldsymbol{x}))(\delta_{kj} + u_{kj}(\boldsymbol{y})). \tag{15}$$

Suppose $G = G'^*$, where G' is an algebraic group, and let u be a rational homomorphism of G' into $GL(n)$. Then, if t is a generic point of G'_0 over K, $u(t)$ is a matrix $(\delta_{ij} + u_{ij}(t))$ where the $u_{ij}(t)$ are elements of the local ring $\mathfrak{o}_K(e, G'_0)$; taking uniformizing parameters and identifying $\mathfrak{O}_K(e, G'_0)$ with a ring of power series, the $u_{ij}(t)$ are identified to power series $\bar{u}_{ij}(\boldsymbol{x})$ and $\boldsymbol{u} = (\bar{u}_{ij}(\boldsymbol{x}))$ is the homomorphism of G into $GL^*(n)$, corresponding to u.

LEMMA 2. *Let $\boldsymbol{u}$ be a homomorphism of a formal Lie group G (over a field K) into $GL^*(n)$, and let H be an algebraic subgroup of $GL(n)$, defined over K. Suppose that H is the set of matrices of coordinates z_{ij} such that $P_\lambda(z_{11}, \cdots, z_{nn}) = 0$, where (P_λ) is a family of polynomials in $K[X_{11}, \cdots, X_{nn}]$. Then, in order that $\boldsymbol{u}(G) \subset H^*$, it is necessary and sufficient that the power series $P_\lambda(u_{11}(\boldsymbol{x}), \cdots, u_{nn}(\boldsymbol{x})) = 0$ for each λ.*

Let $\mathfrak{c}$ be the ideal generated by the P_λ, $\mathfrak{b} \supset \mathfrak{c}$ the ideal of H. We first observe that the condition is equivalent to saying that $P(u_{11}(\boldsymbol{x}), \cdots, u_{nn}(\boldsymbol{x})) = 0$ for every $P \in \mathfrak{b}$, since $P^m \in \mathfrak{c}$ for m large enough and the ring of power series has no divisors of 0. Next, if $\mathfrak{b}_0 \supset \mathfrak{b}$ is the ideal of the connected component H_0 of H, it is also equivalent to say that $P(u_{11}(\boldsymbol{x}), \cdots, u_{nn}(\boldsymbol{x}))$

$=0$ for every $P\in\mathfrak{b}_0$. Indeed, the polynomials $P\in\mathfrak{b}_0$ are characterized by the property that $PQ_0\in\mathfrak{b}$, where Q_0 is a polynomial with nonvanishing constant term [6, p. 86, th. 2], and as the $u_{ij}(\boldsymbol{x})$ have no constant term, it is clear that the power series $Q_0(u_{11}(\boldsymbol{x}),\cdots,u_{nn}(\boldsymbol{x}))$ has a nonvanishing constant term, i. e. is invertible. We can therefore suppose H is *connected.*

The condition is necessary, for if $t=(\delta_{ij}+t_{ij})$ is a generic point of H over K, the t_{ij} belong to $\mathfrak{o}_K(e,H)$, and $P(t_{11},\cdots,t_{nn})=0$ for any $P\in\mathfrak{b}$; let $(s_k)_{1\leq k\leq m}$ be a system of uniformizing parameters of $\mathfrak{o}_K(e,H)$; then $\boldsymbol{u}$ is defined by a system of m power series $v_k(\boldsymbol{x})$, and $u_{ij}(\boldsymbol{x})$ is the series obtained by substituting $v_k(\boldsymbol{x})$ to s_k in the expression of t_{ij} as power series in the s_k, hence $P(u_{11}(\boldsymbol{x}),\cdots,u_{nn}(\boldsymbol{x}))=0$.

To prove the converse, note that $K(t)$ is the field of fractions of the quotient ring $K[X_{11},\cdots,X_{nn}]/\mathfrak{b}=\mathfrak{R}$; let $\bar{X}_{ij}$ be the class $\bmod\,\mathfrak{b}$ of X_{ij} in $\mathfrak{R}$. Then we can write $s_k=P_k(\bar{X}_{11},\cdots,\bar{X}_{nn})/Q_k(\bar{X}_{11},\cdots,\bar{X}_{nn})$, where P_k and Q_k are polynomials of $K[X_{11},\cdots,X_{nn}]$ such that $P_k(0)=0$, $Q_k(0)\neq 0$, the polynomials P_k, Q_k being only determined $\bmod\,\mathfrak{b}$. From the assumption on the $u_{ij}(\boldsymbol{x})$, the elements

$$v_k(\boldsymbol{x})=P_k(u_{11}(\boldsymbol{x}),\cdots,u_{nn}(\boldsymbol{x}))/Q_k(u_{11}(\boldsymbol{x}),\cdots,u_{nn}(\boldsymbol{x}))$$

are well determined power series without constant terms. On the other hand, if w is the natural injection of H into $GL(n)$, there exists a system of uniformizing parameters $(t'_k)_{1\leq k\leq n^2}$ of $\mathfrak{o}_K(e,GL(n))$, such that $s_k=\bar{w}(t'_k)$ for $1\leqq k\leqq m$, and that $\bar{w}(t'_k)=0$ for $k>m$, in other words the t'_k for $k>m$ are in the ideal generated by $\mathfrak{b}$ in the local ring $\mathfrak{o}_K(e,GL(n))$. The t'_k are power series in the coordinates of a generic matrix of $GL(n)$ (which form, as we have seen, a system of uniformizing parameters of $\mathfrak{o}_K(e,GL(n))$); substituting the $u_{ij}(\boldsymbol{x})$ to these coordinates in these power series, we obtain 0 for $k>m$ and $v_k(\boldsymbol{x})$ for $1\leqq k\leqq m$, which shows that the $v_k(\boldsymbol{x})$ define a homomorphism of G into H^* such that $\boldsymbol{u}=\boldsymbol{w}\circ\boldsymbol{v}$.

We will say that a formal Lie group G is *representable* if it is *isogenous to a subgroup of a group $GL^*(n)$*. As we will chiefly be interested in properties invariant under isogeny, we will mainly consider subgroups of $GL^*(n)$.

PROPOSITION 20. *For any formal Lie group G, the center $Z(G)$ is such that $G/Z(G)$ is representable.*

PROPOSITION 21. *For any algebraic group G', $Z(G'^*)=(Z(G'))^*$.*

Both propositions will be proved by the method used by M. Rosenlicht to show that if G' is an algebraic group, $G'/Z(G')$ is isogenous to an algebraic matrix group ([16, p. 432, th. 13]; see also [18]). Let $\boldsymbol{x} = (x_1, \cdots, x_n)$, $\boldsymbol{z} = (z_1, \cdots, z_n)$ be independent generic points of the formal Lie group G, L a perfect field containing the ring $K[[z_1, \cdots, z_n]]$, and $\mathfrak{o}$ the ring of power series $L[[x_1, \cdots, x_n]]$; if $\mathfrak{m}$ is the maximal ideal of $\mathfrak{o}$ (power series without constant terms) then, for any $h > 0$, $\mathfrak{m}^h$ is the ideal of power series having only terms of total degree $\geqq h$. If to each $f \in \mathfrak{m}$ we associate the power series $f_z(\boldsymbol{x}) = f(\boldsymbol{z}^{-1}\boldsymbol{x}\boldsymbol{z})$, it is clear that $f \rightarrow f_z$ maps $\mathfrak{m}^h$ into $\mathfrak{m}^h$, hence defines, for each h, a homomorphism j_z of $\mathfrak{m}/\mathfrak{m}^h$ into itself, such that $j_z j_{z^{-1}} = 1$; j_z is therefore an automorphism of the L-vector space $\mathfrak{m}/\mathfrak{m}^h$. The classes $\bar{\boldsymbol{x}}^\alpha$ of the monomials $\boldsymbol{x}^\alpha$ such that $|\alpha| < h$ form a basis for $\mathfrak{m}/\mathfrak{m}^h$, hence we may write $j_z(\bar{\boldsymbol{x}}^\alpha) = \sum_{|\beta| < h} c_{\alpha\beta}(\boldsymbol{z})\bar{\boldsymbol{x}}^\beta$ for $|\alpha| < h$. It is then clear that $\boldsymbol{z} \rightarrow (c_{\alpha\beta}(\boldsymbol{z}) - \delta_{\alpha\beta})$ is a *homomorphism* $\boldsymbol{u}_h$ of the group G into $GL^*(n_h)$, where $n_h = \dim \mathfrak{m}/\mathfrak{m}^h$. Let Z_h be the kernel of $\boldsymbol{u}_h$; then we have obviously $Z_{h+1} \subset Z_h$, and therefore there is a smallest h such that $Z_k = Z_h$ for all $k \geqq h$. If $\boldsymbol{v}$ is the natural injection of Z_h into G, $\boldsymbol{y}$ a generic point of Z_h, we have therefore $f - f_{\boldsymbol{v}(\boldsymbol{y})} \in \mathfrak{m}^k$ for *any* $k \geqq h$, i.e. $f = f_{\boldsymbol{v}(\boldsymbol{y})}$ for all $f \in \mathfrak{m}$, and this shows by definition that $Z_h \subset Z(G)$. On the other hand, if $\boldsymbol{w}$ is the natural injection of $Z(G)$ into G, and $\boldsymbol{t}$ a generic point of $Z(G)$, we have $f_{\boldsymbol{w}(\boldsymbol{t})} = f$ for all $f \in \mathfrak{m}$, hence $Z(G) \subset Z_k$ for any k, and therefore $Z(G) = Z_h$, and $G/Z(G)$ is isogenous to a subgroup of $GL^*(n_h)$ by Proposition 11, which proves Proposition 20.

Suppose now $G = G'^*$; we define in a similar way (M. Rosenlicht, *loc. cit.*) for any $h \geqq 1$ a rational homomorphism $u_h : s \rightarrow (c'_{\alpha\beta}(s) - \delta_{\alpha\beta})$ of G' into $GL(n_h)$; and if we take a system of uniformizing parameters in $\mathfrak{o}_K(e, G'_0)$ and identify it with $\boldsymbol{z}$, then it follows from the definitions that $c_{\alpha\beta}(\boldsymbol{z})$ is the power series identified to $c'_{\alpha\beta}(s)$ (when s is a generic point of G'_0 over K). In other words, $\boldsymbol{u}_h$ is the homomorphism corresponding to u_h; hence, by Proposition 18, if Z'_h is the kernel of u_h, $Z_h = Z'^*_h$. But (*loc. cit.*) Z'_h is equal to the center $Z(G')$ for sufficiently large h; hence this proves Proposition 21.

16. Algebraic hull of a subgroup of $GL^*(n)$. In what follows, an *algebraic set* in $GL(n)$ will have the same meaning as in [2]. If M is an algebraic set in $GL(n)$, defined over K, $\mathfrak{b}$ its ideal in $K[X_{11}, \cdots, X_{nn}]$, G a formal Lie group over K and $\boldsymbol{u}$ a homomorphism of G into $GL^*(n)$, we say that $\boldsymbol{u}(G)$ is *contained in* M if, for any polynomial $P \in \mathfrak{b}$, the power series $P(u_{11}(\boldsymbol{x}), \cdots, u_{nn}(\boldsymbol{x})) = 0$. It is clear that if H is a subgroup of G (as defined in no. 5), then $\boldsymbol{u}(H) \subset M$. The same argument as in Lemma 2 shows that in order that $\boldsymbol{u}(G) \subset M$ it is sufficient that $P_\lambda(u_{ij}(x)) = 0$ for a family of polynomials $P_\lambda \in K[X_{11}, \cdots, X_{nn}]$ such that M is the set of matrices for which all P_λ are 0.

PROPOSITION 22. *For any homomorphism $\boldsymbol{u}$ of a formal Lie group G over K into $GL^*(n)$, the smallest algebraic set $\mathfrak{A}(G,\boldsymbol{u})$ of $GL(n)$ containing $\boldsymbol{u}(G)$ is a connected subgroup of $GL(n)$, defined over K, and $\boldsymbol{u}(G)$ is contained in the formal Lie group $(\mathfrak{A}(G,\boldsymbol{u}))^*$.*

Let $\mathfrak{b}$ be the ideal of $\mathfrak{A}(G,\boldsymbol{u})$ in $K[X_{11}, \cdots, X_{nn}]$; we prove that if s, t are in $\mathfrak{A}(G,\boldsymbol{u})$ then so is st, which will prove $\mathfrak{A}(G,\boldsymbol{u})$ is a group [6, p. 82, prop. 2]. For any polynomial $P \in K[X_{11}, \cdots, X_{nn}]$, and any $s \in GL(n)$, let ${}_sP$ be the polynomial with coefficients in $K[s]$ obtained by substituting in P to the X_{ij} the coordinates of the matrix, product of s and of the matrix $(\delta_{ij} + X_{ij})$. We can then write

$$(16) \qquad {}_sP(u_{11}(\boldsymbol{y}), \cdots, u_{nn}(\boldsymbol{y})) = \sum_\alpha Q_\alpha(s_{11}, \cdots, s_{nn})\boldsymbol{y}^\alpha$$

where the Q_α are *polynomials* of $K[X_{11}, \cdots, X_{nn}]$ (since a term in $\boldsymbol{y}^\alpha$ can only come from terms of degree $\leqq |\alpha|$ in the $u_{ij}(\boldsymbol{y})$), and the s_{ij} the coordinates of s. Suppose $P \in \mathfrak{b}$; then we have

$$P(u_{11}(\boldsymbol{xy}), \cdots, u_{nn}(\boldsymbol{xy})) = 0$$

which, as $\boldsymbol{u}$ is a homomorphism, is equivalent to

$$\sum_\alpha Q_\alpha(u_{11}(\boldsymbol{x}), \cdots, u_{nn}(\boldsymbol{x}))\boldsymbol{y}^\alpha = 0$$

and implies therefore $Q_\alpha(u_{11}(\boldsymbol{x}), \cdots, u_{nn}(\boldsymbol{x})) = 0$ for each α. But by definition, this means that $Q_\alpha \in \mathfrak{b}$ for each α; hence, if $s \in \mathfrak{A}(G,\boldsymbol{u})$, we have $Q_\alpha(s_{11}, \cdots, s_{nn}) = 0$ for each α, and therefore, by (16), ${}_sP \in \mathfrak{b}^{K(s)}$ (ideal generated by $\mathfrak{b}$ in $K(s)[X_{11}, \cdots, X_{nn}]$); hence $P(st) = 0$ for any $t \in \mathfrak{A}(G,\boldsymbol{u})$, which proves our assertion. The argument in Lemma 2 shows moreover that $\mathfrak{A}(G,\boldsymbol{u})$ is connected, and it also follows from Lemma 2 that $\boldsymbol{u}(G) \subset (\mathfrak{A}(G,\boldsymbol{u}))^*$.

We shall simply write $\mathfrak{A}(\boldsymbol{u}(G))$ instead of $\mathfrak{A}(G,\boldsymbol{u})$, $\mathfrak{A}^*(\boldsymbol{u}(G))$ instead of $(\mathfrak{A}(G,\boldsymbol{u}))^*$; when $\boldsymbol{u}$ is a monomorphism (i.e. $(G,\boldsymbol{u})$ a subgroup of $GL^*(n)$) we will simply write $\mathfrak{A}(G)$ and $\mathfrak{A}^*(G)$. We say that $\mathfrak{A}(G)$ is the *algebraic hull*[14] of $\boldsymbol{u}(G)$ in $GL(n)$. It is clear that if G' is a connected algebraic subgroup of $GL(n)$, $\mathfrak{A}(G'^*) = G'$ and $\mathfrak{A}^*(G'^*) = G'^*$.

---

[14] Here is an example of a formal Lie group $G \subset GL^*(2)$ which is distinct from its

Note that Proposition 22 is also valid when $GL(n)$ is replaced by an algebraic group G' which is an *open subset of an affine space,* the origin of the space being the neutral element of G'; the only modification in the proof is that the Q_α are replaced by rational functions R_α/S_α with $S_\alpha(0) \neq 0$. We shall make use of that remark when G' is a *product* of several groups $GL(n_k)$.

PROPOSITION 23. *If G is a formal Lie subgroup of $GL^*(n)$ and N a normal subgroup in G, then $\mathcal{A}(N)$ is a normal subgroup in $\mathcal{A}(G)$.*

Let $\mathfrak{b}$ be the ideal of $\mathcal{A}(N)$ in $K[X_{11},\cdots,X_{nn}]$; we can suppose that the subgroup N is typical, and then, if $\boldsymbol{x}$ is a generic point of N, $\boldsymbol{z}$ a generic point of G, $\boldsymbol{u}$ the natural injection of G into $GL^*(n)$, we have $P(\boldsymbol{u}(\boldsymbol{z})\boldsymbol{u}(\boldsymbol{x})(\boldsymbol{u}(\boldsymbol{z}))^{-1}) = 0$ for any $P \in \mathfrak{b}$. For any $P \in K[X_{11},\cdots,X_{nn}]$ and any $s \in GL(n)$, let ${}^sP$ be the polynomial with coefficients in $K(s)$ obtained by substituting to the X_{ij} (coordinates of the matrix $X = (\delta_{ij} + X_{ij})$) the coordinates of the matrix sXs^{-1}; we have then ${}^sP(\boldsymbol{u}(\boldsymbol{x})) = P(s\boldsymbol{u}(\boldsymbol{x})s^{-1}) = \sum_\alpha R_\alpha(s_{11},\cdots,s_{nn})\boldsymbol{x}^\alpha$, where the R_α are rational functions defined at the origin. If $P \in \mathfrak{b}$, we have then as in Proposition 22, $R_\alpha(u_{11}(\boldsymbol{z}),\cdots,u_{nn}(\boldsymbol{z})) = 0$, in other words, the numerators of the R_α belong to the ideal $\mathfrak{c}$ of $\mathcal{A}(G)$. This proves that if $s \in \mathcal{A}(G)$, ${}^sP$ belongs to $\mathfrak{b}^{K(s)}$, hence that $sts^{-1} \in \mathcal{A}(N)$ for any $t \in \mathcal{A}(N)$.

PROPOSITION 24. *Let G', G'' be two connected algebraic groups which are open subsets of affine spaces, and f an everywhere defined rational map of G' into G''; suppose $\boldsymbol{u}$ is a homomorphism of a formal Lie group G into G'^*, M an algebraic subset of G'', and that for any polynomial P of the ideal $\mathfrak{b}$ of M, $P(f(\boldsymbol{u}(\boldsymbol{x}))) = 0$. Then $\mathcal{A}(\boldsymbol{u}(G)) \subset f^{-1}(M)$.*

For any generic point $s \in G'$, and any polynomial $P \in \mathfrak{b}$, we have $P(f(s)) = Q(s)/R(s)$ with Q, R polynomials in $K[s]$, and $R(0) \neq 0$, and $f^{-1}(M)$ is the set of matrices for which all the polynomials Q vanish. The remark preceding Proposition 22 then shows that $\boldsymbol{u}(G) \subset f^{-1}(M)$, hence the result.

PROPOSITION 25. a) *If G is a subgroup of $GL^*(n)$, G' a subgroup*

---

algebraic hull $\mathcal{A}(G)$. We take G as the image of the multiplicative group I_0 by the homomorphism

$$x \to \begin{pmatrix} 1+x & 0 \\ 0 & (1+x)^{\zeta} \end{pmatrix}$$

where ζ is a *p-adic integer which is not a rational number* [9, p. 241]. G has therefore dimension 1, whereas from the characterization of the tori in $GL(n)$ [2, §7, pp. 42-46] and the choice of ζ, it follows at once that $\mathcal{A}(G)$ has dimension 2.

of $GL^*(n')$, *then* $\mathfrak{A}(G\times G')=\mathfrak{A}(G)\times\mathfrak{A}(G')$.

b) *If* M,N *are two subgroups of* $GL^*(n)$, *and if* M *centralizes* N, *then* $\mathfrak{A}(M)$ *centralizes* $\mathfrak{A}(N)$.

c) *If* M,N *are two normal subgroups of a subgroup of* $GL^*(n)$, *then* $[\mathfrak{A}(M),\mathfrak{A}(N)]=\mathfrak{A}([M,N])$.

d) *For any subgroup* G *of* $GL^*(n)$, $\mathfrak{A}(D^k(G))=D^k(\mathfrak{A}(G))$ *and* $\mathfrak{A}(C^k(G))=C^k(\mathfrak{A}(G))$.

e) *In order that a subgroup* G *of* $GL^*(n)$ *be commutative* (resp. *solvable, nilpotent*), *it is necessary and sufficient that* $\mathfrak{A}(G)$ *be commutative* (resp. *solvable, nilpotent*).

f) *Let* G *be a subgroup of* $GL^*(n)$, N *a normal subgroup of* G, M *a subgroup of* G *containing* N. *Then if* M/N *is commutative* (resp. *solvable, nilpotent*), $\mathfrak{A}(M)/\mathfrak{A}(N)$ *is commutative* (resp. *solvable, nilpotent*).

These results are the counterparts of (3.2), (3.4), (4.5), (4.6), (4.7) and (4.8) in [2, pp. 33-35]; it will be observed that the proofs of these last results are purely formal consequences of the propositions corresponding to Propositions 22, 23 and 24 above, and of (4.3) in [2, p. 34]; the only point which needs some comment is the inclusion $[M,N]\subset[\mathfrak{A}(M),\mathfrak{A}(N)]^*$ (which is obvious in the context of [2]); this follows here from Proposition 19, which yields $[M,N]\subset[\mathfrak{A}^*(M),\mathfrak{A}^*(N)]=[\mathfrak{A}(M),\mathfrak{A}(N)]^*$, using Proposition 17 and Proposition 23. We omit the rest of the proofs.

THEOREM 4. *For any subgroup* G *of* $GL^*(n)$, $D(G)=\mathfrak{A}^*(D(G))=(D(\mathfrak{A}(G)))^*$, *and any normal subgroup of* G *is also a normal subgroup of* $\mathfrak{A}^*(G)$.

This corresponds to Theorems 13 and 15 of [6, pp. 173 and 177] (and implies them when the characteristic is 0[10]); in non rigorous language, we can say that *the group of commutators of any representable formal Lie group "is algebraic", and is "equal" to the commutator subgroup of the algebraic hull of G.*

The proof is an adaptation of Chevalley's proof of his Theorem 13 (*loc. cit.*). We start with the group law of $GL^*(n)$ defined by (14). By Proposition 4, for any normal subgroup N of G, it is possible to "change variables" in $GL^*(n)$, in other words to find n^2 power series $x'_k=f_k(x_{11},\cdots,x_{nn})$ with nonvanishing jacobian, such that the subgroups $\mathfrak{A}^*(G)$, G and N of $GL^*(n)$ be "defined" respectively by the equations $x'_k=0$ for $k>m$, $x'_k=0$ for $k>q$, $x'_k=0$ for $k>r$ $(r\leqq q\leqq m)$. Let

$x_{ij} = g_{ij}(x'_1, \cdots, x'_{n^2})$ be the "inverse" system of power series. Let $\boldsymbol{y} = (y_1, \cdots, y_r)$ be a generic point of N; denote by $\boldsymbol{g}(\boldsymbol{y})$ the matrix whose coordinates are the g_{ij} in which x'_k has been replaced by y_k for $k \leqq r$, by 0 for $k > r$, and consider, for a matrix s of coordinates s_{ij}, the power series $f_k(s\boldsymbol{g}(\boldsymbol{y})s^{-1})$ obtained by replacing in f_k the x_{ij} by the coordinates of the matrix $s\boldsymbol{g}(\boldsymbol{y})s^{-1}$; it is clear that we have $f_k(s\boldsymbol{g}(\boldsymbol{y})s^{-1}) = \sum\limits_{\alpha} R_{k\alpha}(s_{11}, \cdots, s_{nn})\boldsymbol{y}^{\alpha}$, where the $R_{k\alpha} = P_{k\alpha}/Q_{k\alpha}$ are *rational* functions of $K(X_{11}, \cdots, X_{nn})$ such that $Q_{k\alpha}(0) \neq 0$. Now let $\boldsymbol{z} = (z_1, \cdots, z_q)$ be a generic point of G, $\boldsymbol{g}(\boldsymbol{z})$ the matrix whose coordinates are the g_{ij} in which x'_k is replaced by z_k for $k \leqq q$, by 0 for $k > q$. From the assumption that N is normal in G, it follows that for $k > r$, the power series $f_k(\boldsymbol{g}(\boldsymbol{z})\boldsymbol{g}(\boldsymbol{y})\boldsymbol{g}(\boldsymbol{z})^{-1})$ are 0, in other words that $R_{k\alpha}(\boldsymbol{g}(\boldsymbol{z})) = 0$ for all $k > r$ and all α. But by definition, this implies that $R_{k\alpha}(s_{11}, \cdots, s_{nn}) = 0$ if $s \in \mathfrak{A}(G)$; if $\boldsymbol{t} = (t_1, \cdots, t_m)$ is a generic point of $\mathfrak{A}^*(G)$, $\boldsymbol{g}(\boldsymbol{t})$ the matrix whose coordinates are the g_{ij} in which x'_k is replaced by t_k for $k \leqq m$, by 0 for $k > m$, we have therefore $R_{k\alpha}(\boldsymbol{g}(\boldsymbol{t})) = 0$ for all $k > r$ and all α, hence $f_k(\boldsymbol{g}(\boldsymbol{t})\boldsymbol{g}(\boldsymbol{y})\boldsymbol{g}(\boldsymbol{t})^{-1}) = 0$ for $k > r$, which means of course that N is a *normal* subgroup of $\mathfrak{A}^*(G)$.

Take now $N = D(G)$, which is therefore a normal subgroup of $\mathfrak{A}^*(G)$. With the same conventions as above, consider the power series

$$f_k(s\boldsymbol{g}(\boldsymbol{z})s^{-1}\boldsymbol{g}(\boldsymbol{z})^{-1}) = \sum_{\alpha} S_{k\alpha}(s_{11}, \cdots, s_{nn})\boldsymbol{z}^{\alpha},$$

where the $S_{k\alpha}$ are again *rational* functions. By assumption,

$$f_k(\boldsymbol{g}(\boldsymbol{z}')\boldsymbol{g}(\boldsymbol{z})\boldsymbol{g}(\boldsymbol{z}')^{-1}\boldsymbol{g}(\boldsymbol{z})^{-1}) = 0 \text{ for } k > r,$$

when $\boldsymbol{z}' = (z'_1, \cdots, z'_q)$ is a second generic point of G; this means that $S_{k\alpha}(\boldsymbol{g}(\boldsymbol{z}')) = 0$ for all $k > r$ and all α, and we conclude as above that $f_k(s\boldsymbol{g}(\boldsymbol{z})s^{-1}\boldsymbol{g}(\boldsymbol{z})^{-1}) = 0$ for $k > r$ and $s \in \mathfrak{A}(G)$, hence

$$f_k(\boldsymbol{g}(\boldsymbol{t})\boldsymbol{g}(\boldsymbol{z})\boldsymbol{g}(\boldsymbol{t})^{-1}\boldsymbol{g}(\boldsymbol{z})^{-1}) = 0 \text{ for } k > r.$$

Consider finally the power series $f_k(\boldsymbol{g}(\boldsymbol{t})s\boldsymbol{g}(\boldsymbol{t})^{-1}s^{-1}) = \sum\limits_{\alpha} T_{k\alpha}(s_{11}, \cdots, s_{nn})\boldsymbol{t}^{\alpha}$ with rational $T_{k\alpha}$; the same argument proves that

$$f_k(\boldsymbol{g}(\boldsymbol{t})\boldsymbol{g}(\boldsymbol{t}')\boldsymbol{g}(\boldsymbol{t})^{-1}\boldsymbol{g}(\boldsymbol{t}')^{-1}) = 0 \text{ for } k > r,$$

when $\boldsymbol{t}' = (t'_1, \cdots, t'_m)$ is a second generic point of $\mathfrak{A}^*(G)$. As we know that $D(G)$ is a normal subgroup of $\mathfrak{A}^*(G)$, we conclude that $D(\mathfrak{A}^*(G)) \subset D(G)$; but clearly $D(G) \subset D(\mathfrak{A}^*(G))$, hence $D(G) = D(\mathfrak{A}^*(G))$. Now from Proposition 19 it follows that $D(\mathfrak{A}^*(G)) = (D(\mathfrak{A}(G)))^*$, and from Proposition 25 d), $D(\mathfrak{A}(G)) = \mathfrak{A}(D(G))$, whence $D(G) = \mathfrak{A}^*(D(G))$.

17. Normalizers and centralizers.

PROPOSITION 26. *Let G be a formal Lie group over K, M, N two subgroups of G. Then there is a largest subgroup P of M such that, if $\mathbf{u}$ is the natural injection of P into G, $\mathbf{i}_{u(z)}(N_{(L)}) \subset N_{(L)}$, where $\mathbf{z}$ is a generic point of P and L a perfect field containing $K[[\mathbf{z}]]$.*

Let $\mathbf{x} = (x_1, \cdots, x_n)$ be a generic point of G, and suppose N is a typical subgroup defined by $x_i = 0$ for $i > q$. Let $\mathbf{y} = (y_1, \cdots, y_m)$ be a generic point of M, E a perfect field containing $K[[\mathbf{y}]]$, $\mathfrak{o}$ the ring of power series $E[[\mathbf{x}]]$, $\mathfrak{m}$ the maximal ideal of $\mathfrak{o}$. As in Proposition 20, we define an automorphism j_y of the E-vector space $\mathfrak{m}/\mathfrak{m}^h$ by associating to each $f \in \mathfrak{m}$ the power series $f_y(\mathbf{x}) = f(\mathbf{v}(\mathbf{y})^{-1}\mathbf{x}\mathbf{v}(\mathbf{y}))$ ($\mathbf{v}$ natural mapping of M into G), and taking classes $\bmod \mathfrak{m}^h$; and with the same notations as in Proposition 20, we may write $j_y(\bar{\mathbf{x}}^\alpha) = \sum_{|\beta|<h} c_{\alpha\beta}(\mathbf{y})\mathbf{x}^\beta$, thus obtaining a homomorphism $\mathbf{w}_h$: $\mathbf{y} \to (c_{\alpha\beta}(\mathbf{y}) - \delta_{\alpha\beta})$ of M into $GL^*(n_h)$. Let J be the interval $1 \leqq i \leqq q$, and let V_h be the subspace of $\mathfrak{m}/\mathfrak{m}^h$ having as a basis the $\mathbf{x}^\alpha$ such that $\alpha \in \mathbf{N}^J$. It is clear that the set of matrices $s \in GL(n_h)$ such that $s(V_h) \subset V_h$ is an algebraic subgroup S_h of $GL(n_h)$. Let Q_h be the connected component of the identity in the algebraic group $S_h \cap \mathfrak{A}(\mathbf{w}_h(M))$; in the formal Lie group $\mathfrak{A}^*(\mathbf{w}_h(M))$, $\mathbf{w}_h(M)$ is a normal subgroup by Theorem 4, hence the g. l. b. $Q^*_h \wedge \mathbf{w}_h(M)$ is defined (Proposition 9), and therefore we can also define the inverse image $P_h = \mathbf{w}^{-1}_h(Q^*_h)$ in M (see remark at the end of no. 8). These definitions imply that P_h is the *largest* subgroup of M such that $j_{f(t)}(V_h) \subset V_h$, if $\mathbf{t}$ is a generic point of P_h and $\mathbf{f}$ the natural mapping of P_h into M. Furthermore, from that definition it follows that $P_{h+1} \subset P_h$, hence there is an integer r such that $P_h = P_r$ for $h \geqq r$, and $P = P_r$ obviously satisfies the requirements of Proposition 26.

When $M = G$, the subgroup P obviously contains N, and is the largest subgroup of G such that N is a normal subgroup of P; we say, as usual, that P is the *normalizer* of N in G. Proposition 26 then expresses the fact that for any subgroup M of G, the g. l. b. $P \wedge M$ *exists*. This enables us to prove the result announced in no. 5, namely:

THEOREM 5. *The subgroups of a formal Lie group G form a complete lattice.*

Owing to the chain conditions, all we need to do is to prove that $H_1 \wedge H_2$ exists for any pair of subgroups of G. Consider the normalizer N_2 of H_2 in G; any subgroup contained in H_1 and H_2 is contained in H_1

and N_2, hence in $H_1 \wedge N_2$, which is defined as we have seen above. Moreover, in the group N_2, H_2 is a normal subgroup, hence $H_2 \wedge (H_1 \wedge N_2)$ is defined (Proposition 9), and is obviously the g. l. b. of H_1 and H_2.

COROLLARY 1. *Let* $\boldsymbol{u}$ *be a surjective homomorphism of* G *onto a formal Lie group* G', H_1, H_2 *two subgroups of* G, H'_1, H'_2 *two subgroups of* G'; *then*

$$\boldsymbol{u}(H_1 \vee H_2) = \boldsymbol{u}(H_1) \vee \boldsymbol{u}(H_2) \tag{17}$$

$$\begin{aligned} \boldsymbol{u}^{-1}(H'_1 \vee H'_2) &= \boldsymbol{u}^{-1}(H'_1) \vee \boldsymbol{u}^{-1}(H'_2), \\ \boldsymbol{u}^{-1}(H'_1 \wedge H'_2) &= \boldsymbol{u}^{-1}(H'_1) \wedge \boldsymbol{u}^{-1}(H'_2). \end{aligned} \tag{18}$$

Formulae (18) follow at once from the fact that $H' \to \boldsymbol{u}^{-1}(H')$ is a one-to-one inclusion preserving correspondence between subgroups of G' and subgroups of G containing the kernel N of $\boldsymbol{u}$ (Proposition 11); the same argument proves (17), when we observe that

$$H_1 \vee H_2 \vee N = (H_1 \vee N) \vee (H_2 \vee N),$$

and that $\boldsymbol{u}(H) = \boldsymbol{u}(H \vee N)$ for any subgroup H of G.

COROLLARY 2. *Let* H_1, H_2 *be two algebraic subgroups of* $GL(n)$, $H_1 \vee H_2$ (resp. $H_1 \wedge H_2$) *the smallest algebraic subgroup of* $GL(n)$ *containing* H_1 *and* H_2 (resp. *the largest algebraic subgroup of* $GL(n)$ *contained in* H_1 *and* H_2). *Then* $(H_1 \wedge H_2)^* = H^*_1 \wedge H^*_2$, *and, if* H_1 *and* H_2 *are connected,* $(H_1 \vee H_2)^* = H^*_1 \vee H^*_2$.

Note that $H_1 \wedge H_2$ is the set theoretic intersection $H_1 \cap H_2$, and is defined over K if both H_1 and H_2 are. We have obviously $(H_1 \wedge H_2)^* \subset H^*_1 \wedge H^*_2$; on the other hand $\mathfrak{a}(H^*_1 \wedge H^*_2)$ is contained in both $\mathfrak{a}(H^*_1)$ and $\mathfrak{a}(H^*_2)$, which are respectively the connected components of e in H_1 and H_2; hence $H^*_1 \wedge H^*_2$ is contained in the connected component of $H_1 \wedge H_2$, which proves that $H^*_1 \wedge H^*_2 \subset (H_1 \wedge H_2)^*$ by definition. On the other hand, we have obviously $H^*_1 \vee H^*_2 \subset (H_1 \vee H_2)^*$. To prove the converse inclusion, we remark that if x_i $(1 \leqq i \leqq m)$ are independent generic points of H_1, y_i $(1 \leqq i \leqq m)$ independent generic points of H_2, over a common field of definition K, then, if m is large enough, $x_1y_1x_2y_2 \cdots x_my_m$ is a generic point of $H_1 \vee H_2$ over K; this is easily proved as the Lemmas 3.1 and 4.3 of [2]. The rest of the argument is then practically identical to that in Proposition 19, and we accordingly suppress it.

PROPOSITION 27. *For any subgroup* H *of a formal Lie group* G, *there is a largest subgroup* H' *which commutes with* H (no. 11). *That subgroup*

H' (called the *centralizer* of H in G) *is a normal subgroup of the normalizer of* H.

With the notations of Proposition 26 (H replacing N and G replacing M), we consider the algebraic subgroup T_h of $GL(n_h)$ consisting of the matrices s such that the restriction of s to V_h is the identity, and the inverse image $\boldsymbol{w}^{-1}{}_h(T^*{}_h)$ in G. These subgroups form a decreasing sequence of subgroups of G, and their intersection is the group H'. If N is the normalizer of H in G, it is clear that $H' \subset N$. To prove H' is normal in N, we may suppose $N = G$. Then, if $\boldsymbol{z}$ is a generic point of G, $\boldsymbol{i}_{\boldsymbol{z}}(H'_{(L)})$ commutes with $\boldsymbol{i}_z(H_{(L)})$ (L perfect field containing $K[[\boldsymbol{z}]]$), and as the latter is equal to $H_{(L)}$ we have by definition $\boldsymbol{i}_{\boldsymbol{z}}(H'_{(L)}) \subset H'_{(L)}$.

For representable groups, we have additional results. For any $s \in GL(n)$, let a_s be the rational map $t \rightarrow sts^{-1}$ of $GL(n)$ onto itself, defined over the field $\boldsymbol{F}_p(s)$; it gives rise to an automorphism $\boldsymbol{a}_s$ of the formal Lie group $(GL^*(n))_{(\boldsymbol{F}_p(s))}$.

PROPOSITION 28. *Let G be a subgroup (over a field K) of $GL^*(n)$; the set of elements $s \in GL(n)$ such that $\boldsymbol{a}_s(G_{(K(s))}) \subset G_{(K(s))}$* (resp. *such that the restriction of $\boldsymbol{a}_s$ to $G_{(K(s))}$ is the identity mapping*) *is an algebraic subgroup $\mathfrak{N}(G)$* (resp. *$\mathfrak{Z}(G)$*) *of $GL(n)$, defined over K and such that $\mathfrak{N}^*(G) = (\mathfrak{N}(G))^*$* (resp. *$\mathfrak{Z}^*(G) = (\mathfrak{Z}(G))^*$*) *is the normalizer* (resp. *centralizer*) *of G in $GL^*(n)$.*

First, for reasons of dimension, if $\boldsymbol{a}_s(G_{(K(s))}) \subset G_{(K(s))}$, both groups are equal, from which it follows that if $s \in \mathfrak{N}(G)$, then $s^{-1} \in \mathfrak{N}(G)$; if $t \in \mathfrak{N}(G)$ and $L = K(s,t)$, we have $\boldsymbol{a}_s(G_{(L)}) = G_{(L)}$ and $\boldsymbol{a}_t(G_{(L)}) = G_{(L)}$; as $\boldsymbol{a}_{st} = \boldsymbol{a}_s \circ \boldsymbol{a}_t$, we have $\boldsymbol{a}_{st}(G_{(L)}) = G_{(L)}$, hence $st \in \mathfrak{N}(G)$, and $\mathfrak{N}(G)$ is therefore a group. On the other hand, taking G to be a typical subgroup of $GL^*(n)$ by a suitable "change of variables," the same argument as in Theorem 4 proves that the elements $s \in \mathfrak{N}(G)$ are characterized as the matrices satisfying a family of equations $R_{k\alpha}(s_{11}, \cdots, s_{nn}) = 0$, where the $R_{k\alpha}$ are rational functions of $K(X_{11}, \cdots, X_{nn})$. Lastly, if H is a subgroup of $GL^*(n)$, $\boldsymbol{z}$ a generic point of H and $\boldsymbol{u}$ the natural mapping of H into $GL^*(n)$, then the condition $\boldsymbol{i}_{\boldsymbol{u}(\boldsymbol{z})}(G_{(E)}) \subset G_{(E)}$ (for a perfect field E containing $K[[z]]$) is equivalent to the relations $R_{k\alpha}(u_{11}(\boldsymbol{z}), \cdots, u_{nn}(\boldsymbol{z})) = 0$ for all indices, and the fact that $\mathfrak{N}^*(G)$ is the normalizer of G in $GL^*(n)$ then follows from Lemma 2. A similar proof applies to the centralizer.

COROLLARY 1. *For any normal subgroup N of G, $\mathfrak{A}(G)$ is contained in $\mathfrak{N}(N)$.*

This follows from the first part of the proof of Theorem 4.

COROLLARY 2. *$\mathfrak{N}(G)$ is contained in the normalizer of the algebraic hull $\mathfrak{A}(G)$ in $GL(n)$, and $\mathfrak{Z}(G)$ is equal to the centralizer of $\mathfrak{A}(G)$ in $GL(n)$.*

The first statement follows from Proposition 23, applied to the normal subgroup G of $\mathfrak{N}^*(G)$; the second follows likewise from Proposition 25 b) and from the fact that $\mathfrak{Z}(G)$ is a decreasing function of G.

18. Solvable representable groups. Let G be a solvable subgroup of $GL^*(n)$; then by Proposition 25 e), $\mathfrak{A}(G)$ is solvable. We denote by $\mathfrak{T}(n)$ the subgroup of *triangular* matrices $s = (s_{ij})$ (with $s_{ij} = 0$ for $i > j$), by $\mathfrak{U}(n)$ the normal subgroup of $\mathfrak{T}(n)$ consisting of *unipotent* triangular matrices (i.e. with diagonal elements 1). Applying the preceding remark and the Lie-Kolchin theorem [2, th. 10.4], we have the corresponding result for representable groups:

PROPOSITION 29. *If G is a solvable subgroup of $GL^*(n)$ defined over an algebraically closed field K, there is an element $s \in GL(n)$, rational over K, such that $\mathbf{a}_s(G) \subset \mathfrak{T}^*(n)$.*

In other words, if $\mathbf{u}$ is the natural mapping of G into $GL^*(n)$, and $\mathbf{v} = \mathbf{a}_s \circ \mathbf{u}$, then the matrix $1 + \mathbf{v}(\mathbf{z}) = (v_{ij}(\mathbf{z}) + \delta_{ij})$ is triangular ($\mathbf{z}$ being a generic point of G).

PROPOSITION 30. *For any solvable formal Lie group G, the derived group $D(G)$ is nilpotent.*

This follows immediately from Proposition 29 if G is a subgroup of $GL^*(n)$, for we can then suppose that $G \subset \mathfrak{T}^*(n)$, and $D(G) \subset D(\mathfrak{T}^*(n)) \subset \mathfrak{U}^*(n)$; as $\mathfrak{U}(n)$ is a nilpotent algebraic group, $\mathfrak{U}^*(n)$ is nilpotent by the corollary to Proposition 19. In general, if G is solvable, $G/Z(G)$ is solvable and representable, hence $D(G/Z(G))$ is nilpotent; but $D(G/Z(G))$ is isogenous to $D(G)/(Z(G) \wedge D(G))$ by Propositions 16 and 11, hence a fortiori $D(G)/Z(D(G))$, which is isogenous to a quotient group of $D(G)/(Z(G) \wedge D(G))$, is nilpotent. But this implies that $C^k(D(G)) \subset Z(D(G))$ for some k (corollary to Proposition 16); by definition, we have $C^{k+1}(D(G)) = \mathbf{e}$, hence $D(G)$ is nilpotent.

We next prove the result corresponding to A. Borel's conjugation theorem for maximal solvable subgroups:

PROPOSITION 31. *Let G be a subgroup of $GL^*(n)$, over an algebraically closed field K. Then:*

a) *If S_1, S_2 are any two maximal solvable subgroups of G, there is an $s \in \mathfrak{A}(G)$, rational over K, such that $\boldsymbol{a}_s(S_1) = S_2$.*

b) *Any maximal solvable subgroup of G has the form $R^* \wedge G$, where R is a maximal connected solvable subgroup of $\mathfrak{A}(G)$; and conversely.*

a) $\mathfrak{A}(S_1)$ and $\mathfrak{A}(S_2)$ are solvable connected subgroups of $\mathfrak{A}(G)$ by Proposition 25 e), defined over K, hence contained in maximal solvable connected subgroups R_1 and R_2 defined over K. By the conjugation theorem [2, Th. 16. 5, p. 66, and Prop. 16. 10, p. 68], there is an $s \in \mathfrak{A}(G)$, rational over K, such that $sR_1s^{-1} = R_2$; replacing S_1 by $\boldsymbol{a}_s(S_1)$ (and using cor. 1 to Prop. 28), we can suppose that $R_1 = R_2$, and therefore S_1 and S_2 are contained in the solvable subgroup R^*_1 (cor. to Prop. 19). As both are maximal in G, if they were distinct, neither would be contained in the other, hence $S_1 \vee S_2$ would be distinct from S_1 and S_2; but as $S_1 \vee S_2$ is contained in the solvable group R^*_1, it would be solvable, contrary to definition.

b) If S is a maximal solvable subgroup of G, it follows as in a) that it is contained in R^*, where R is a maximal connected solvable subgroup of $\mathfrak{A}(G)$; as $R^* \wedge G$ is solvable, it must be S. Conversely, let R be a maximal connected solvable subgroup of $\mathfrak{A}(G)$; if $R^* \wedge G$ were not maximal, it would be properly contained in a maximal solvable subgroup S_1 of G, which in turn would be of the form $R^*_1 \wedge G$ where R_1 is a maximal connected solvable subgroup of $\mathfrak{A}(G)$. Then there is $s \in \mathfrak{A}(G)$, rational over K, such that $R = sR_1s^{-1}$, hence $\boldsymbol{a}_s(S_1) \subset R^*$; as $\dim S_1 > \dim S$, $S \vee \boldsymbol{a}_s(S_1)$, which is contained in R^*, would be a solvable subgroup of G properly containing S, contrary to the assumption that $S = R^* \wedge G$.

I have not been able to determine if the algebraic hull $\mathfrak{A}(S)$ of S in G is a maximal solvable connected subgroup of $\mathfrak{A}(G)$.[15]

If G is an arbitrary formal Lie group, S a maximal solvable subgroup of G, then S contains the center $Z(G)$; for if f is the natural epimorphism of G onto $G' = G/Z(G)$, $S' = f(S)$ is solvable, and $S'' = f^{-1}(S')$ is such that $S''/Z(G)$, isogenous to S', is solvable; hence S'' is solvable, and as $S'' \supset S$, it must be equal to S. The same argument proves that S' is a maximal solvable subgroup of $G/Z(G)$ and that conversely the inverse image of a maximal solvable subgroup of $G/Z(G)$ is a maximal solvable subgroup of G. I do not know if the l. u. b. of all maximal solvable subgroups of G is equal to G; however, the derived group $D(G')$ is isogenous to a group H^*, where H is a connected algebraic matrix group (Theorem 4), and the l. u. b.

---

[15] This is related to another unsolved question: is the center $Z(S)$ equal to the center $Z(G)$ for a maximal solvable subgroup S (cf. [2, p. 72, prop. 18. 5]) ?

of the maximal solvable connected subgroups of H is H itself [2, Th. 17.4, p. 71]; hence the maximal solvable subgroups of G' have a l.u.b. which contains $D(G')$ (cor. 2 to Th. 5), from which it follows that *the* l.u.b. *of the maximal solvable subgroups of* G *contains* $D(G) \vee Z(G)$. A question which remains unsettled for general formal Lie groups is whether any two maximal solvable subgroups are isomorphic; all which follows from Proposition 31 and the preceding remarks is that their quotients by $Z(G)$ are isomorphic, and therefore they have same dimension.

PROPOSITION 32. *If S is a maximal solvable subgroup of a formal Lie group G, S is equal to its normalizer in G.*

Let N be the normalizer of S in G; if $N' = N/S$ is commutative, then N is solvable, which implies $N = S$ by definition. If not, as $D(N') \neq \mathbf{e}$, there are solvable subgroups $S' \subset N'$ not reduced to $\mathbf{e}$, and the inverse image S_1 of S' in N is then solvable, since S_1/S and S are solvable; this is a contradiction, hence $N = S$.

19. Maximal tori. We will say a formal Lie group G is a *torus* if it is isomorphic to a direct product $I_0{}^m$ of multiplicative groups. It follows immediately from [9, p. 236, Th. 3] that any subgroup and any quotient group of a torus is a torus.

LEMMA 3.[16] *Let N be a normal subgroup of a formal Lie group G, containing the center $Z(G) = Z$ and such that N/Z is a torus. Then $N = Z$.*

Using Proposition 4, we can suppose that the group law of G is pseudo-canonical, and that both subgroups Z and N are typical; more precisely, if m, q and n are the dimensions of Z, N and G, and if we denote by I, J and H the intervals $1 \leqq i \leqq n$, $1 \leqq i \leqq m$, $1 \leqq i \leqq q$, the X_α or Z_α of the structural basis of $\mathfrak{G}$ such that $\alpha \in \mathbf{N}^J$ (resp. $\alpha \in \mathbf{N}^H$) form the structural basis of the subhyperalgebra $\mathfrak{Z}$ (resp. $\mathfrak{N}$) of the group Z (resp. N). We first prove that if $i \in H - J$, then X_{0i} commutes with any element Y of $\mathfrak{g}_0$. As N is a normal subgroup, we have $[X_{0i}, Y] \in \mathfrak{g}_0 \cap \mathfrak{N}$ (cor. 1 to Th. 2); on the other hand, the class $\bar{X}_{0i}$ of X_{0i} modulo the normal ideal $\mathfrak{a}(\mathfrak{Z})$ is in the Lie algebra of the torus N/Z, hence we may assume it is such that $\bar{X}^p{}_{0i} = \bar{X}_{0i}$ [9, p. 233, prop. 5]; this means that $X^p{}_{0i} - X_{0i}$ belongs to the intersection of $\mathfrak{a}(\mathfrak{Z})$ and $\mathfrak{g}_0$, i.e. to $\mathfrak{g}_0 \cap \mathfrak{Z}$, which is contained in the center of the Lie algebra $\mathfrak{g}_0$. Hence we have $[X^p{}_{0i} - X_{0i}, Y] = 0$, or

$$[X_{0i}, Y] = [X^p{}_{0i}, Y] = [X_{0i}, [X_{0i}, [\cdot\cdot\cdot [X_{0i}, Y] \cdot\cdot\cdot]]]$$

---

[16] Lemma 3 and its corollary are not true for formal Lie groups over a field of characteristic 0.

by Jacobson's formula. Now, N/Z being commutative, we see as above that $[U,V]\in\mathfrak{g}_0\cap\mathfrak{Z}$ for any two elements of the Lie algebra $\mathfrak{g}_0\cap\mathfrak{N}$; the previous formula then proves, first that $[X_{0i},Y]$ is in $\mathfrak{g}_0\cap\mathfrak{Z}$, and then that it is 0.

As a basis for induction, suppose now we have proved that all elements X_{hi} such that $h<r$ and $i\in H-J$ are in the center of the algebra $\mathfrak{z}_{r-1}$; the same is true therefore for all X_α of height $h(\alpha)<r$, such that $\alpha\in N^H$, and also (by Lemma 1) for the Z_α of corresponding indices. We now proceed in several steps.

(i) We first prove that $[X_{ri},Y]=[X^p{}_{ri},Y]$ *for* $i\in H-J$, $Y\in\mathfrak{z}_{r-1}$. The difference $X^p{}_{ri}-X_{ri}$ belongs to the Lie-p-algebra $\mathfrak{g}_r\cap\mathfrak{N}$, and applying to it the iterated homomorphism p'^r shows that $X^p{}_{ri}-X_{ri}=S+T$, where $S\in\mathfrak{g}_r\cap\mathfrak{Z}$ and $T\in\mathfrak{z}_{r-1}\cap\mathfrak{N}$; the result follows from the fact that $[S,Y]=0$ by definition and $[T,Y]=0$ by the inductive hypothesis.

(ii) Next we show that $[X_{ri},X_{0j}]=0$ *for* $i\in H-J$ *and for any* $j\in I$. The inductive hypothesis first proves, as in the proof of Theorem 3, that $[X_{ri},X_{0j}]^\circ-1\otimes[X_{ri},X_{0j}]-[X_{ri},X_{0j}]\otimes 1=0$, i.e. that $[X_{ri},X_{0j}]$ *is in* $\mathfrak{g}_0$; on the other hand, $[X_{ri},X_{0j}]$ is in the normal ideal $\mathfrak{a}(\mathfrak{N})$, hence in $\mathfrak{g}_0\cap\mathfrak{N}$. But then $[X^p{}_{ri},X_{0j}]$ is in the normal ideal $\mathfrak{a}(\mathfrak{Z})$ by Jacobson's formula and the commutativity of N/Z, and on the other hand it is in $\mathfrak{g}_0$ by (i) and by what has just been proved; therefore $[X_{ri},X_{0j}]\in\mathfrak{g}_0\cap\mathfrak{Z}$, and then Jacobson's formula yields $[X^p{}_{ri},X_{0j}]=0$, which proves our contention by (i).

(iii) We can now prove that $[X_{ri},Y]=0$ *for* $i\in H-J$, $Y\in\mathfrak{z}_{r-1}$. We can of course suppose $Y=Z_\alpha$ with $h(\alpha)<r$, and we use induction on $|\alpha|$, the result being proved in (ii) for $|\alpha|=1$. As in (ii), the induction hypothesis first shows that $[X_{ri},Z_\alpha]^\circ-1\otimes[X_{ri},Z_\alpha]-[X_{ri},Z_\alpha]\otimes 1=0$, hence $[X_{ri},Z_\alpha]\in\mathfrak{g}_0$. Then $[X^p{}_{ri},Z_\alpha]=0$ by (ii) and Jacobson's formula, and we conclude by (i).

(iv) The next step is to show that $[X_{0i},X_{rj}]=0$ *for* $i\in H-J$ *and any* $j\in I$. As we have $X^p{}_{0i}-X_{0i}\in\mathfrak{Z}$, $[X_{0i},X_{rj}]=[X^p{}_{0i},X_{rj}]$; on the other hand, the inductive hypothesis proves as above that $[X_{0i},X_{rj}]\in\mathfrak{g}_0$; Jacobson's formula then yields the result.

(v) Now we prove by induction on $h<r$, that $[X_{hi},X_{rj}]=0$ *for* $i\in H-J$ *and any* $j\in I$. From Lemma 1 and the inductive hypothesis, it follows that $[Z_\alpha,X_{rj}]=0$ for $\alpha\in N^H$ and $h(\alpha)<h$. As before, this implies that $[X_{hi},X_{rj}]\in\mathfrak{g}_0$. But as in (i) we remark that $X^p{}_{hi}-X_{hi}=S+T$, where $S\in\mathfrak{g}_h\cap\mathfrak{Z}$ and $T\in\mathfrak{z}_{h-1}\cap\mathfrak{N}$; the inductive hypothesis then proves that $[X_{hi},X_{rj}]=[X^p{}_{hi},X_{rj}]$, and the conclusion follows as usual from Jacobson's formula.

(vi) We can now take the final step and prove that $[X_{ri}, X_{rj}] = 0$ *for* $i \in H - J$ *and any* $j \in I$. From (ii) and (v) it follows that X_{ri} commutes with all elements of $\mathfrak{s}_{r-1}$ and X_{rj} with all elements of $\mathfrak{s}_{r-1} \cap \mathfrak{N}$; the usual argument implies that $[X_{ri}, X_{rj}] \in \mathfrak{g}_0$. On the other hand, as $X^p_{ri} - X_{ri} = S + T$, with $S \in \mathfrak{g}_r \cap \mathfrak{Z}$ and $T \in \mathfrak{s}_{r-1} \cap \mathfrak{N}$, we have $[X_{ri}, X_{rj}] = [X^p_{ri}, X_{rj}]$ by (v), and (ii) and Jacobson's formula end the proof. The induction on r is thus completed, and shows that every element of the hyperalgebra $\mathfrak{N}$ commutes with every element of $\mathfrak{G}$, which concludes the proof of Lemma 3.

COROLLARY. *A torus N which is a normal subgroup of G is contained in the center.*

For $(N \vee Z)/Z$ is isogenous to a quotient group of N (Proposition 11), hence a torus, and $N \vee Z$ is a normal subgroup of G, so that we can apply Lemma 3.

PROPOSITION 33. *If G is a torus in $GL^*(n)$ over an algebraically closed field, then $\mathfrak{A}(G)$ is a torus in $GL(n)$.*

From Proposition 25 e), we know that $\mathfrak{A}(G)$ is commutative and connected, and by [2, p. 53, Th. 11.1] $\mathfrak{A}(G)$ is the direct product of a torus C_s and a unipotent abelian group C_u. Let v be the (rational) projection of $\mathfrak{A}(G)$ onto C_u, with kernel C_s; then the corresponding homomorphism $\boldsymbol{v}$ of $\mathfrak{A}^*(G)$ onto C^*_u has kernel C^*_s (Proposition 18), and as C^*_u is unipotent, $\boldsymbol{v}(G) = \boldsymbol{e}$ [9, p. 240, Th. 4], which proves that $G \subset C^*_s$, in other words $\mathfrak{A}(G) = C_s$, q. e. d.

PROPOSITION 34. *Let G be a subgroup of $GL^*(n)$, over an algebraically closed field K. Then:*

a) *If T_1, T_2 are any two maximal tori of G, there is an $s \in \mathfrak{A}(G)$ rational over K, such that $\boldsymbol{a}_s(T_1) = T_2$.*

b) *Any maximal torus of G has the form $R^* \wedge G$, where R is a maximal torus in $\mathfrak{A}(G)$; and conversely.*

c) *Any maximal torus in a maximal solvable subgroup of G is a maximal torus in G.*

The proofs of a) and b) run exactly parallel to the proofs in Proposition 31, using Proposition 33 and [2, cor. 16. 6, p. 67] instead of [2, Th. 16. 5]; they can therefore be omitted. Statement c) follows at once from b) and from the corresponding statement in [2, cor. 16. 6].

Here again, it remains to be seen if, for a maximal torus T of G, $\mathfrak{A}(T)$ is a maximal torus in $\mathfrak{A}(G)$ (cf. cor. to Proposition 38). For a general formal Lie group G, let T be a maximal torus of $G/Z(G)$; if we apply Lemma 3 to the group $f^{-1}(T)$, where f is the natural epimorphism of G onto $G/Z(G)$, we see that $f^{-1}(T)$ is *commutative*, hence is the product of a unique torus T_0, its *core* [9, p. 236, Th. 3], and of its p-radical U; moreover, U is contained in $Z(G)$ by [9, p. 240, Th. 4], and $T=f(T_0)$. Conversely, if T'_0 is any maximal torus in G, $f(T'_0)$ is a torus in $G/Z(G)$, and if it was properly contained in a torus T in $G/Z(G)$, the preceding argument would show that T'_0 is properly contained in a torus in $f^{-1}(T)$. We therefore deduce from Proposition 34 that *all maximal tori in a formal Lie group G over an algebraically closed field are isomorphic.* Furthermore:

PROPOSITION 35. *In a formal Lie group G over an algebraically closed field, the intersection of all maximal tori of G is the core of the center of G.*

From the preceding remarks, and Proposition 34 b), we see that the intersection C of the maximal tori of G is contained in $f^{-1}(D^* \wedge G')$, where f is a homomorphism of G into a group $GL^*(n)$, with kernel $Z(G)$, and D the intersection of all maximal tori of the group $\mathfrak{A}(G')$. But, by [2, p. 71, Prop. 18.1], D is a torus contained in the center of $\mathfrak{A}(G')$, hence $D^* \wedge G'$ is a torus contained in the center of G', and by Lemma 3, $f^{-1}(D^* \wedge G')$ is contained in the center of G, q. e. d.

20. Nilpotent groups and Cartan subgroups. We say that a formal Lie group G is *unipotent* if there exists a power p^k of the characteristic such that $x^{p^k}=e$ (which means $\phi^{(p^k)}(x)=e$, if we define, by induction on h, the system $\phi^{(h)}(x)$ of n power series as equal to $\phi(x,\phi^{(h-1)}(x))$).

PROPOSITION 36. *Any unipotent formal Lie group G is nilpotent.*

It is clear that the representable group $G'=G/Z(G)$ is unipotent. If u is a monomorphism of G' into a group $GL^*(m)$, and z a generic point for G', the matrix $u(z)$ is unipotent. As the set of unipotent matrices in $GL(m)$ is defined by a system of algebraic equations, we conclude that $\mathfrak{A}(G')$ is a group of unipotent matrices, hence is nilpotent [2, p. 74, Th. 19.4]. Therefore G' is nilpotent, and so is of course G.

PROPOSITION 37. *A representable nilpotent group G over an algebraically closed field is quasi-direct product of its unique maximal torus and of its unique maximal unipotent subgroup.*

We can suppose G is a subgroup of a group $GL^*(n)$. Then $\mathfrak{A}(G)$ is nilpotent, hence [2, p. 53, Th. 11.1] the direct product of its unique maximal torus C and its unique maximal unipotent subgroup U. It is clear that $D(\mathfrak{A}(G)) = D(U)$. The group $D^*(U)$ is equal to $D(G)$ (Theorem 4), and the abelian group $G/D(G)$ is thus contained in the group $C^* \times (U^*/D(U^*))$. Now $G/D(G)$ is the direct product of its core H and its p-radical R, and as C^* is a torus and $U^*/D(U^*)$ a unipotent abelian group, we have $H \subset C^*$ and $R \subset U^*/D(U^*)$ [9, p. 240, Th. 4], which shows in particular that R is a unipotent group. The inverse image V of R in G contains $D(G) = D(U^*)$, and as R and $D(U^*)$ are unipotent, so is V, and therefore, by the same argument as in Proposition 36, we have $V \subset U^*$; moreover $V = G \wedge U^*$, since $V \subset G \wedge U^*$, and if this was a proper inclusion, the dimension of the p-radical of $G/D(G)$ would be strictly greater than that of R. A similar argument shows that if f is the projection of $\mathfrak{A}(G)$ onto U, $f(G) = V$, hence G is contained in the direct product $V \times C^*$, and as it contains V, it is equal to $V \times (G \wedge C^*)$; as $G \wedge C^* = T$ is the maximal torus of G (Proposition 34 b)), the proof is complete.

Proposition 37 applies in particular to *abelian* representable groups; it shows at once that (in contrast with Ado's theorem for formal Lie groups over a field of characteristic 0) there exist *non representable* abelian groups. This is for instance the case for all one-dimensional groups I_r $(0 < r < +\infty)$ [9, p. 229, Th. 2], for I_0 is the only one-dimensional torus and $W_1 = I_\infty$ (the additive group) the only unipotent one-dimensional group. Similarly, all *simple* abelian groups of dimension > 1 [11, pp. 450-451] are non-representable, by Propositions 36 and 37; this shows incidentally that if a simple abelian group S of dimension > 1 is contained in a formal Lie group G, it is contained *in the center* of G. It is clear that if two subgroups H_1, H_2 of a formal Lie group G are such that there is *no* homomorphism of H_1 nor of H_2 into a group $GL^*(n)$ which is not trivial (such groups may be called *totally nonrepresentable groups*, and the previous examples are of that kind), then $H_1 \vee H_2$ has the same property. There is therefore a *largest* totally non-representable group N, contained of course in the center of G. It would be interesting to know the structure of N and if N is a quasi-direct factor of G.

THEOREM 6. *In order that a formal Lie group G over an algebraically closed field K be nilpotent, it is necessary and sufficient that it contain a unique maximal torus, which is then in the center of G.*

a) The *necessity* of the condition follows from Proposition 37 if G is representable. In general, $G/Z(G)$ is nilpotent with G, hence contains a unique maximal torus T which is in its center. But as T is normal in $G/Z(G)$, its inverse image $f^{-1}(T)$ by the natural mapping f of G onto

$G/Z(G)$ is a normal subgroup of G containing $Z(G)$ and whose quotient by $Z(G)$ is a torus; hence $f^{-1}(T) = Z(G)$ by Lemma 3, which means T is reduced to $\boldsymbol{e}$, and the unique maximal torus of G is the core of $Z(G)$.

b) To prove *sufficiency*, let us first assume G is a subgroup of a group $GL^*(n)$, and let T be the unique maximal torus of G. Then, by Proposition 34 a), for any $s \in \mathfrak{A}(G)$, rational over K, $\boldsymbol{a}_s(T) = T$; as the points of $\mathfrak{A}(G)$ which are rational over K are dense in $\mathfrak{A}(G)$, we see that $\mathfrak{A}(G)$ is contained in $\mathfrak{N}(T)$, and therefore T is a normal subgroup in $\mathfrak{A}^*(G)$ (and of course in G). From the corollary to Lemma 3, we conclude that T is in the center of $\mathfrak{A}^*(G)$, hence $\mathfrak{A}(T)$ is in the center of $\mathfrak{A}(G)$ by Proposition 25 b). Furthermore, from Proposition 34 b), any maximal torus S of $\mathfrak{A}(G)$ is such that $S^* \wedge G = T$, and this implies that $S \supset \mathfrak{A}(T)$, otherwise the connected component of $S \cap \mathfrak{A}(T)$ would have strictly smaller dimension than $\mathfrak{A}(T)$ and contain T, contrary to the definition of $\mathfrak{A}(T)$. There is a rational homomorphism g of $\mathfrak{A}(G)$ into a group $GL(m)$, with kernel $\mathfrak{A}(T)$ [2, p. 40, Lemma 5.10.2], and the maximal tori of the algebraic group $H = g(\mathfrak{A}(G))$ are the images $g(S)$ where S is a maximal torus of $\mathfrak{A}(G)$ [2, p. 80, Th. 22.1]. If $G' = \boldsymbol{g}(G)$, H is equal to $\mathfrak{A}(G')$, otherwise the inverse image of $\mathfrak{A}(G')$ by g would contain G and be properly contained in $\mathfrak{A}(G)$, contrary to definition. Furthermore, we have $G' \wedge \boldsymbol{g}(S^*) = \boldsymbol{e}$; indeed $G' \vee \boldsymbol{g}(S^*) = \boldsymbol{g}(G \vee S^*)$ and as $G \vee S^*$ contains the kernel $\mathfrak{A}^*(T)$ of $\boldsymbol{g}$, we have $\dim(G' \vee \boldsymbol{g}(S^*)) = \dim(G \vee S^*) - \dim \mathfrak{A}^*(T)$. But as $G \wedge S^* = T$, $\dim(G \vee S^*) = \dim G + \dim S^* - \dim T$ by Proposition 11 (G being normal in $\mathfrak{A}^*(G)$), hence

$$\begin{aligned}\dim(G' \vee \boldsymbol{g}(S^*)) &= (\dim G - \dim T) + (\dim S^* - \dim \mathfrak{A}^*(T)) \\ &= \dim G' + \dim \boldsymbol{g}(S^*),\end{aligned}$$

which proves by Proposition 11 that $\dim(G' \wedge \boldsymbol{g}(S^*)) = 0$ (G' being normal in H). Now it is enough to prove that G' is nilpotent, since T is in the center of G; the preceding argument thus allows us to restrict ourselves to the case in which $T = \boldsymbol{e}$.

We are actually going to prove that in such a case $\mathfrak{A}(G)$ (hence also G) is a *unipotent* group. First there is no maximal torus in $D(G)$, which by Theorem 4 is equal to $(D(\mathfrak{A}(G))^*$; by [2, p. 67, cor. 16.7], the algebraic group $D(\mathfrak{A}(G))$ is unipotent. Let f be a rational homomorphism of $\mathfrak{A}(G)$ into a group $GL(m)$, with kernel $D(\mathfrak{A}(G))$ [2, p. 40, Lemma 5.10.2]; it will be enough to prove that the algebraic abelian group $H = f(\mathfrak{A}(G))$ is unipotent. Suppose the contrary: then, by [2, p. 53, Th. 11.1], H is the direct product of its unique maximal torus C and its unique maximal unipotent subgroup U, and by assumption $C \neq \{e\}$. Furthermore, the abelian formal Lie group $f(G)$ is a subgroup of H^*, and a direct product of its core $Q \subset C^*$ and its p-radical $R \subset U^*$ [9, p. 240, Th. 4]. If we had $Q = \boldsymbol{e}$, $f(G)$ would be contained in U^*, hence G would be contained in the algebraic group $f^{-1}(U)$, which is properly contained in $\mathfrak{a}(G)$, contrary to the definition of $\mathfrak{a}(G)$. We have therefore $\dim Q > 0$. Consider now the algebraic subgroup $C_0 = f^{-1}(C)$ of $\mathfrak{a}(G)$, which is such that C_0^* contains the normal subgroup $Q_0 = f^{-1}(Q)$ of G. If S is a maximal torus of H, $f(S)$ is a maximal torus of H [2, p. 80, Th. 22.1] hence equal of C, which proves that $S \subset C_0$. We are going to show that $S^* \wedge Q_0$ is not reduced to $\boldsymbol{e}$, which is a contradiction by the assumption and by Proposition 34b). As we have $f(S^* \vee Q_0) = C^* \vee Q = C^*$, we have $\dim C^* = \dim(S^* \vee Q_0) - \dim D(G) = \dim S^*$, since $S^* \wedge D(G) = \boldsymbol{e}$. This, by Proposition 11, yields $\dim(S^* \wedge Q_0) = \dim Q_0 - \dim D(G) = \dim Q > 0$, and we have reached the desired conclusion.

Suppose now G is an arbitrary formal Lie group having a unique maximal torus T; then, if $\boldsymbol{u}$ is the natural epimorphism of G onto $G/Z(G)$, $\boldsymbol{u}(T)$ is the unique maximal torus T_0 of $G/Z(G)$, and by the preceding argument, $G/Z(G)$ is nilpotent, hence also G. Furthermore, $\boldsymbol{u}^{-1}(T_0)$ is normal in G and its quotient by $Z(G)$ is a torus; therefore Lemma 3 proves that actually $T_0 = \boldsymbol{e}$, $T \subset Z(G)$ and $G/Z(G)$ is *unipotent*. I do not know if T is then a quasi-direct factor of G.

PROPOSITION 38. *Let G be a representable solvable formal Lie group over an algebraically closed field. Then there is a largest unipotent subgroup G_u of G, which is normal in G, and for any maximal torus T of G, $G = T \vee G_u$ and $G_u \wedge T = \boldsymbol{e}$.*

We suppose $G \subset GL^*(n)$. Consider the derived group $D(G)$, which is nilpotent (Proposition 30) and equal to $(D(\mathfrak{a}(G)))^*$ (Theorem 4). There is a rational homomorphism f of $\mathfrak{a}(G)$ into a group $GL(m)$, with kernel $D(\mathfrak{a}(G))$, and $f(G)$ is an abelian representable group, which is therefore direct product of its core C and its p-radical R, which is unipotent (Proposition 37). Let $N = f^{-1}(R) \supset D(G)$; this is a solvable normal subgroup of G. Moreover, if S is a maximal torus in N, we have $f(S) = \boldsymbol{e}$, and $S \subset D(G)$. But as $D(G)$ is nilpotent, it has a unique maximal torus, and so therefore has N, which proves, by Theorem 6, that N is nilpotent. N is therefore, by Proposition 37, quasi-direct product of its largest unipotent subgroup G_u and its unique maximal torus S. Furthermore, if V is a

11 and 2 that there is a homomorphism $\boldsymbol{v}_1$ (resp. $\boldsymbol{v}_2$) of G onto a group G_1 (resp. G_2) isogenous to H_1 (resp. H_2), with kernel H_2 (resp. H_1). Consider the homomorphism $\boldsymbol{v}=(\boldsymbol{v}_1,\boldsymbol{v}_2)$ of G into $G_1 \times G_2$; we have $\boldsymbol{v}(H_1)=G_1$ and $\boldsymbol{v}(H_2)=G_2$, hence $\boldsymbol{v}(G)$ contains $G_1 \vee G_2 = G_1 \times G_2$; $\boldsymbol{v}$ is thus surjective, and as G and $G_1 \times G_2$ have same dimension by Proposition 11, $\boldsymbol{v}$ is an *isogeny*. Let $\boldsymbol{w}$ be an isogeny of $G_1 \times G_2$ onto some group $G^{(t)}$ (prop. 2), such that $\boldsymbol{w}\circ\boldsymbol{v}=\boldsymbol{p}^t$; $\boldsymbol{w}^{(-t)}$ is then an isogeny of $G_1{}^{(-t)} \times G_2{}^{(-t)}$ onto G, mapping $G_1{}^{(-t)}$ onto H_1 and $G_2{}^{(-t)}$ onto H_2. The last statement of the proposition is obvious from the definition of a quasi-direct product.

The preceding definition and proof can of course be extended in an obvious way to any finite number of factors. For an example of a quasi-direct product which is not a direct product, see no. 21.

13. Subgroup of commutators; ascending and descending central series. Let N_1, N_2 be two normal subgroups of G, $\boldsymbol{u}$ a homomorphism of G into a group H, P the kernel of $\boldsymbol{u}$. In order that the subgroups $\boldsymbol{u}(N_1)$ and $\boldsymbol{u}(N_2)$ commute in H, the corresponding subhyperalgebras of $\mathfrak{H}$ must commute elementwise (prop. 12). Using Propositions 6 and 7, we have an equivalent condition by restricting ourselves to the case in which $\boldsymbol{u}$ is the natural epimorphism $\boldsymbol{g}$ of G onto G/P. But then the subhyperalgebra corresponding to $\boldsymbol{g}(N_1)$ (resp. $\boldsymbol{g}(N_2)$) consists of the classes of the elements of $\mathfrak{N}_1$ (resp. $\mathfrak{N}_2$) modulo the normal ideal $\mathfrak{a}(\mathfrak{P})$ (th. 2); hence, for $T_1 \in \mathfrak{N}_1$, $T_2 \in \mathfrak{N}_2$, $[T_1, T_2]$ must belong to $\mathfrak{a}(\mathfrak{P})$, and conversely.

PROPOSITION 14. *If N_1, N_2 are two normal subgroups*[9] *of G, there exists a smallest normal subgroup $P=[N_1, N_2]$ of G such that the natural images of N_1 and N_2 in G/P commute; $[N_1, N_2]$ is contained in $N_1 \wedge N_2$, and $\mathfrak{a}(\mathfrak{P})$ is the smallest normal ideal containing the alternants $[T_1, T_2]$ where $T_1 \in \mathfrak{N}_1$ and $T_2 \in \mathfrak{N}_2$.*

Once the existence of a smallest P is proved, the characterization of $\mathfrak{a}(\mathfrak{P})$ becomes obvious. As N_1 and N_2 are normal subgroups, $[T_1, T_2]$ belongs both to $\mathfrak{a}(\mathfrak{N}_1)$ and $\mathfrak{a}(\mathfrak{N}_2)$, hence $P \subset N_1 \wedge N_2$ by Proposition 10. Finally, owing to the chain conditions, all we have to prove is that if P_1, P_2 are kernels of homomorphisms $\boldsymbol{g}_1, \boldsymbol{g}_2$ of G into groups H_1, H_2, such that $\boldsymbol{g}_i(N_1)$ and $\boldsymbol{g}_i(N_2)$ commute $(i=1,2)$, then $P_1 \wedge P_2$ has the same property. But $P_1 \wedge P_2$ is the kernel of the homomorphism $\boldsymbol{g}=(\boldsymbol{g}_1,\boldsymbol{g}_2)$ of G into $H_1 \times H_2$, and it is clear that $\boldsymbol{g}(N_1)$ and $\boldsymbol{g}(N_2)$ commute in $H_1 \times H_2$.

---

[9] There does not seem to be any obvious definition of $[H_1, H_2]$ when H_1, H_2 are arbitrary subgroups of a formal Lie group G.

We will denote by $[\mathfrak{N}_1, \mathfrak{N}_2]$ the hyperalgebra of $[N_1, N_2]$. If g is the natural epimorphism of G onto $G/[N_1, N_2]$, then $g(x_1 x_2 x^{-1}_1 x^{-1}_2) = e$ for any two (independent) generic points x_1 of N_1, x_2 of N_2; if $[N_1, N_2]$ is brought into typical form, being defined by the annulation of all coordinates of index $i > m$, then the coordinates of such indices of $x_1 x_2 x^{-1}_1 x^{-1}_2$ are 0.

In particular, for any normal subgroup N of G, $[N, N]$ is the smallest normal subgroup *in* G such that $N/[N, N]$ be *abelian.* We call $[G, G]$ *the commutator subgroup* or *derived subgroup* of G, and write it $D(G)$ (and its subhyperalgebra $D(\mathfrak{G})$).

PROPOSITION 15. *For any normal subgroup N of G, $[N, N] = D(N)$.*

All we have to show is that $D(N)$ is a normal subgroup *in* G. Now, if z is a generic point of G, and L a perfect extension of $K[[z]]$, i_z is an automorphism of $N_{(L)}$, hence $H = i_z(D(N_{(L)}))$ is a normal subgroup of $N_{(L)}$ such that $N_{(L)}/H$ is abelian. By definition, this implies $H \supset D(N_{(L)})$), and as the two groups have same dimension, they are equal.

We can define as usual the *derived series* of successive commutator subgroups $D^n(G) = D(D^{n-1}(G))$ for $n > 1$, and the *descending central series* $C^1(G) = D(G)$, $C^n(G) = [G, C^{n-1}(G)]$ for $n > 1$.

PROPOSITION 16. *If u is a surjective homomorphism of G onto G', and N_1, N_2 two normal subgroups of G, then $[u(N_1), u(N_2)] = u([N_1, N_2])$.*

Indeed, if $\mathfrak{a} = \mathfrak{a}([\mathfrak{N}_1, \mathfrak{N}_2])$ the image $u'(\mathfrak{a})$ is a normal ideal in $\mathfrak{G}'$ containing all the $[u'(T_1), u'(T_2)] = u'([T_1, T_2])$ for $T_1 \in \mathfrak{N}_1$, $T_2 \in \mathfrak{N}_2$. Conversely, if $\mathfrak{a}' \subset \mathfrak{G}'$ is a normal ideal containing these elements, $u'^{-1}(\mathfrak{a}')$ is a normal ideal in $\mathfrak{G}$ containing the $[T_1, T_2]$, hence contains $\mathfrak{a}$ by definition and therefore $u'(\mathfrak{a})$ is the smallest normal ideal in $\mathfrak{G}'$ containing the $[u'(T_1), u'(T_2)]$.

COROLLARY. *If u is a surjective homomorphism of G onto G', then $u(D^n(G)) = D^n(G')$, $u(C^n(G)) = C^n(G')$.*

PROPOSITION 17. *Let M_1, M_2 be two normal subgroups of G, H a subgroup of G, N_1, N_2 two normal subgroups of H such that $N_1 \subset M_1$, $N_2 \subset M_2$. Then $[N_1, N_2] \subset [M_1, M_2]$.*

Indeed, if g is the natural mapping of G onto $G/[M_1, M_2]$, $g(M_1)$ and $g(M_2)$ commute, hence also $g(N_1) \subset g(M_1)$ and $g(N_2) \subset g(M_2)$; the kernel $H \wedge [M_1, M_2]$ of the restriction of g to H thus contains $[N_1, N_2]$.

COROLLARY. *For any subgroup H of G,*

$$D^n(H) \subset D^n(G) \text{ and } C^n(H) \subset C^n(G).$$

unipotent subgroup of G, and g the natural homomorphism of G onto G/N (which is isogenous to C, hence a torus), we have $g(V) \subset G/N$, hence as $g(V)$ is unipotent, $g(V) = e$, $V \subset N$, and finally $V \subset G_u$; and as G_u is the largest unipotent subgroup of G, it is normal in G. Let now T be any maximal torus of G; $T \wedge N$ is a torus in N, hence contained in S; on the other hand, S being the largest torus in the normal subgroup N, is a normal subgroup of G. In the group $T \vee S$, S is a normal subgroup such that $(T \vee S)/S$ is a torus (isogenous to $T/(T \wedge S)$), and Lemma 3 and its corollary prove that $T \vee S$ is a torus, hence $S \subset T$ by definition. Furthermore we have $T \wedge N = S$ and $T \wedge G_u = e$; finally $f(T)$ is contained in C, hence equal to C for reasons of dimension, hence $g(T) = G/N$, $T \vee G_u = G$.

COROLLARY. *The algebraic group* $\mathfrak{A}(T)$ *is a maximal torus in* $\mathfrak{A}(G)$, *and* $\mathfrak{A}(G_u)$ *is the largest unipotent subgroup of* $\mathfrak{A}(G)$.

Indeed, $\mathfrak{A}(G_u)$ is a normal unipotent subgroup of $\mathfrak{A}(G)$, $\mathfrak{A}(T)$ a torus in $\mathfrak{A}(G)$, hence $\mathfrak{A}(T) \cdot \mathfrak{A}(G_u)$ is an algebraic subgroup of $\mathfrak{A}(G)$ which obviously contains G, hence $\mathfrak{A}(G) = \mathfrak{A}(T) \cdot \mathfrak{A}(G_u)$; as the intersection of a torus and a unipotent subgroup only contains the identity, this proves our assertion.

Note that if R is a maximal solvable subgroup of a representable formal Lie group G, then the largest unipotent subgroup of R is also a maximal unipotent subgroup of G, as follows from the conjugation theorem (Proposition 31).

PROPOSITION 39. *In a formal Lie group G over an algebraically closed field, let T be a maximal torus. The normalizer C of T is also the centralizer of T, and it is a maximal nilpotent subgroup of G, equal to its normalizer in G; moreover, any maximal solvable subgroup of G containing T contains C. Conversely, any nilpotent subgroup H of G which is equal to its normalizer in G is the centralizer of a maximal torus of G.*

We closely follow the proofs of the corresponding results of A. Borel [2, p. 67, cor. 16.8 and p. 76, Lemma 20.6]. It follows at once from the corollary to Lemma 3 that C is also the centralizer of T in G; moreover, if N is the normalizer of C in G, T being the unique maximal torus of the normal subgroup C of N, is a normal subgroup of N, hence $N = C$. From the uniqueness of the maximal torus in C it follows (Theorem 6) that C is nilpotent. C is contained in a maximal solvable subgroup R of G; if G is representable, it follows from that remark and from the conjugation theorems (Propositions 31 and 34) that any maximal solvable subgroup of G containing T contains C. That result is easily extended to the general case, remembering the one-to-one correspondence between maximal solvable subgroups (resp. maximal tori) of G and of $G/Z(G)$. Finally, if Q is a nilpotent subgroup containing C, T is the unique maximal torus of Q, hence in the center of Q, which proves that $Q = C$.

To prove the converse, let us first suppose G is a subgroup of $GL^*(n)$. Then H is direct product of its unique maximal torus S and its largest unipotent subgroup H_u (Proposition 37). Consider a maximal solvable subgroup R of G containing H, and let Q be a maximal torus of R containing S. Let M be the centralizer of S *in* R, which contains H and Q; the largest unipotent subgroup M_u of the solvable group M then contains H_u and we have $M = M_u \vee Q$ by Proposition 38. If we had $H_u \neq M_u$, the normalizer N of H_u in M_u would be different from H_u; this is seen by the same argument as in [2, p. 75, Lemma 20.3], which we suppress. But then, if $\mathbf{f}$ is the natural mapping of M onto M/S, $\mathbf{f}(H_u)$ would be normal in $\mathbf{f}(N)$ and distinct from $\mathbf{f}(N)$ for reasons of dimension, since $S \wedge N = \mathbf{e}$; hence, by Proposition 11, $H = S \vee H_u$ would be normal in $S \vee V$ and distinct from that group, contrary to assumption. Therefore $H_u = M_u$, and as M/M_u is abelian (Proposition 38), H contains the derived group $D(M)$, hence is normal in M; but the hypothesis then implies $H = M$, hence $Q = S$, and S is equal to a maximal torus of R, hence of G (Proposition 34c)). If now C is the centralizer of S *in* G, it is the direct product of S by its largest unipotent subgroup $C_u \supset H_u$. If we had $H_u \neq C_u$, it would follow as above that H would be distinct from its normalizer in G, hence $H = C$, and the proof is complete in that case.

Finally, if G is not representable, it is clear that a subgroup of G equal to its normalizer must contain the center $Z(G)$; but in the one-to-one correspondence between subgroups of $G/Z(G)$ and subgroups of G containing $Z(G)$, nilpotent groups correspond to nilpotent groups and normalizers to normalizers: the image of H in $G/Z(G)$ is thus the normalizer (or centralizer) of a maximal torus T of $G/Z(G)$, and as we know that T is the image of a maximal torus T_0 of G, H is the normalizer of T_0.

We say that the centralizers of maximal tori in G are the *Cartan subgroups* of G.

COROLLARY. *Let G be a subgroup of $GL^*(n)$, over an algebraically closed field K. Then, if C_1, C_2 are any two Cartan subgroups of G, there is an $s \in \mathfrak{A}(G)$, rational over K, such that $\mathbf{a}_s(C_1) = C_2$.*

This follows immediately from Proposition 34a).

If G is a subgroup of $GL^*(n)$, over an algebraically closed field, the relation between the algebraic hull $\mathfrak{A}(C)$ of a Cartan subgroup C of G and the Cartan subgroups of $\mathfrak{A}(G)$ is not clear; nor do we know if the l. u. b. of all Cartan subgroups of G is equal to G.

21. Semisimple and simple formal Lie groups. We say that a formal Lie group G is *semisimple* if it contains no abelian normal subgroup distinct from the identity. A *simple* Lie group is obviously semisimple if it is not abelian.

THEOREM 7. *If G is a semisimple* (resp. *non abelian simple*) *Lie group over a field K, then G is isogenous to a group G'^*, where G' is a semisimple* (resp. *non abelian simple*) *algebraic group of matrices defined over K. Conversely, if G' is a semisimple* (resp. *non abelian simple*) *algebraic group of matrices, G'^* is a semisimple* (resp. *non abelian simple*) *formal Lie group.*

If G is a semisimple Lie group, $Z(G)=\boldsymbol{e}$ by definition, hence G is representable. Among all isogenies $\boldsymbol{u}$ of G into groups $GL^*(n)$, consider one for which the dimension of $\mathfrak{A}(\boldsymbol{u}(G))$ is *minimum*. If G is semisimple, $\mathfrak{A}(\boldsymbol{u}(G))$ cannot have an algebraic abelian normal subgroup N of dimension >0 defined over K; for there would then be a rational homomorphism f of $\mathfrak{A}(\boldsymbol{u}(G))$ into a group $GL(m)$, defined over K, with kernel N [2, p. 40, Lemma 5.10.2]; as $N^* \wedge \boldsymbol{u}(G)$ is an abelian normal subgroup of $\boldsymbol{u}(G)$, it must be reduced to $\boldsymbol{e}$, hence the restriction of f to $\boldsymbol{u}(G)$ is an isogeny, and $f\circ\boldsymbol{u}$ would be an isogeny of G into $GL^*(m)$, such that the dimension of $\mathfrak{A}(f(\boldsymbol{u}(G)))$ would be at most $\dim\mathfrak{A}(\boldsymbol{u}(G))-\dim N<\dim\mathfrak{A}(\boldsymbol{u}(G))$, which contradicts our choice of $\boldsymbol{u}$. The same argument proves that if G is simple and non abelian, $\mathfrak{A}(\boldsymbol{u}(G))$ has no algebraic normal subgroup of dimension >0, defined over K, other than itself. Moreover, in this last case, $D(\mathfrak{A}(G))=\mathfrak{A}(G)$, hence, by Theorem 4, $\boldsymbol{u}(G)=\mathfrak{A}^*(G)$. The same argument holds also in the case of a semisimple group G, as it follows from results of Chevalley [7] that an algebraic connected semisimple group is equal to its derived subgroup.

Suppose conversely G' is a semisimple connected algebraic group of matrices. If G'^* contained an abelian normal subgroup N of dimension >0, $\mathfrak{A}(N)$ would be an abelian normal subgroup of G' of dimension >0 (Proposition 23), hence $N=\boldsymbol{e}$, G'^* is semisimple. Similarly, if G' is simple, and G'^* contains a normal subgroup N of dimension >0, $\mathfrak{A}(N)$ is a normal subgroup of G' of dimension >0, hence equal to G'. But, by Theorem 4, $D(N)$ is then equal to $(D(G'))^*$, hence to G'^*, and this proves that $N=G'^*$, in other words G'^* is a simple formal Lie group.

C. Chevalley has recently succeeded in determining all algebraic semisimple groups of matrices over an algebraically closed field [7]; in particular, it follows from his results that the simple algebraic groups over such a field are those of the Cartan-Killing classification. This fundamental theorem, joined to Theorem 7, shows that all simple nonabelian formal Lie groups over an algebraically closed field are known *up to an isogeny.* It remains to determine what are the possible isogenies between simple groups; when the Lie algebra is simple, only the trivial isogenies $\boldsymbol{p}^t$ exist [8, p. 115, Theorem 7]; but it is known that some of the Lie algebras of the simple algebraic groups are not simple for certain values of the characteristic [14], and it seems likely that this phenomenon corresponds to the existence of nontrivial isogenies. I am not at present in a position to prove this conjecture in every case (actually, the structure of the Lie algebras of the groups of types E_6, E_7, E_8 and F_4 is not even yet determined over a field of arbitrary characteristic), and all I will do here is to show that it is substantiated[17] in the case of the groups of type A_n.

Let us consider the Lie algebra $\mathfrak{gl}(n)$ of the group $GL^*(n)$, and write X_{ij} its basis elements, instead of $X_{0,ij}$ $(1 \leqq i, j \leqq n)$. We have on one hand in $GL^*(n)$ the unimodular group $SL^*(n)$, which is the kernel of the homomorphism f, defined by $f((x_{ij})) = \det(\delta_{ij} + x_{ij}) - 1$ of $GL^*(n)$ into the multiplicative group I_0; it is readily verified that the Lie algebra $\mathfrak{sl}(n)$ of $SL^*(n)$ is the subalgebra of $\mathfrak{gl}(n)$ consisting of the elements $\sum_{i,j} \xi_{ij} X_{ij}$ such that $\sum_{i=1}^{n} \xi_{ii} = 0$. On the other hand, the center Z of $GL^*(n)$ is the image of I_0 by the homomorphism g such that $g_{ij}(x) = \delta_{ij} x$ $(1 \leqq i, j \leqq n)$ (Proposition 21); its Lie algebra $\mathfrak{z}$ is the subalgebra of $\mathfrak{gl}(n)$ generated by the element $X_{11} + \cdot \cdot \cdot + X_{nn}$. Now it is clear that Z is not contained in $SL^*(n)$, hence $Z \wedge SL^*(n) = \boldsymbol{e}$ since Z is one-dimensional, and from Proposition 11 it follows that $Z \vee SL^*(n) = GL^*(n)$; therefore $GL^*(n)$ is the quasi-direct product of its normal subgroups Z and $SL^*(n)$ (Proposition 13). If n is not a multiple of the characteristic p, $\mathfrak{gl}(n)$ is the direct sum of $\mathfrak{z}$ and $\mathfrak{sl}(n)$, hence (Propositions 1 and 13) $GL^*(n)$ is the direct product of Z and $SL^*(n)$. But if n is a multiple of p, we have $\mathfrak{z} \subset \mathfrak{sl}(n)$, and the restriction to $SL^*(n)$ of the natural mapping of $GL^*(n)$ onto the quotient group $PGL^*(n) = GL^*(n)/Z$ is a *non trivial isogeny* $\boldsymbol{u}$. More precisely, $\mathfrak{z}$ is the kernel of $\boldsymbol{u}'$ in $\mathfrak{sl}(n)$, and it is known [14] that the quotient Lie-p-algebra $\mathfrak{sl}(n)/\mathfrak{z}$ is *simple* unless $p = n = 2$. From the homomorphism theorem it then follows that the Lie algebra of $PGL^*(n)$ has an (n^2-2)-dimensional ideal isomorphic to $\mathfrak{sl}(n)/\mathfrak{z}$ [8, p. 116]. This shows that the Lie algebras of $SL^*(n)$ and $PGL^*(n)$ *are not isomorphic* when p divides n and $n \neq 2$; direct computation leads to the same conclusion when $n=2=p$. This provides examples to some situations discussed earlier: $\boldsymbol{u}$ is composed of the natural epimorphism of $GL^*(n)$ onto $PGL^*(n)$ and of the natural monomorphism of $SL^*(n)$ into $GL^*(n)$, but fails to be separable (cf. no. 4); the example $F=SL^*(n)$, $N=Z$ shows that $F/(F \wedge N)$ is not always isomorphic to $(F \vee N)/N$ (no. 10); and the two Jordan-Hölder sequences $GL^*(n) \supset SL^*(n) \supset \boldsymbol{e}$, $GL^*(n) \supset Z \supset \boldsymbol{e}$ have quotient groups which are *not* isomorphic (no. 10).

---

[17] This example has been pointed out to me by J. P. Serre.

As a last remark, let us observe that it follows from Chevalley's result mentioned above that the simple Lie-p-algebras over an algebraically closed field, discovered and studied in recent years by several authors (see e.g. [1] and [15]), which are not isomorphic to Lie algebras of the groups of the Cartan-Killing classification, *cannot correspond to formal Lie groups.* For some of these algebras it is possible to see this directly without using Chevalley's deep results. For instance, consider the *Witt algebra* $\mathfrak{w}$ (the first one to be discovered) over an algebraically closed field K of characteristic $p>0$: it is defined as the algebra of derivations of the associative algebra $\mathfrak{A}=K[X]/(X^p)$ over K and has dimension p. It is known [15] that $\mathfrak{w}$ is simple if $p>2$, and that its group of automorphisms is *solvable* if $p \geqq 5$, But if $\mathfrak{w}$ was the Lie algebra of a formal Lie group G, G would be simple and non abelian [8, p. 115, Theorem 7], hence of the form G'^* by Theorem 7, where G' is an algebraic simple connected group of matrices. Consider now the automorphisms $\boldsymbol{a}_s$ of G, where s ranges over the rational points of G' over K; the restriction $\boldsymbol{f}_s$ of $\boldsymbol{a}'_s$ to the Lie algebra $\mathfrak{g}_0=\mathfrak{w}$ of G would be an automorphism of $\mathfrak{w}$, and $s \rightarrow \boldsymbol{f}_s$ a rational homomorphism (over K) of the group Γ of all elements of G' rational over K, into the group L of all automorphisms of $\mathfrak{w}$. Now L is an algebraic matrix K-group, and so is Γ; the homomorphism $s \rightarrow \boldsymbol{f}_s$ gives rise to a homomorphism of the Lie algebra $\mathfrak{w}$ of Γ into the Lie algebra $\mathfrak{l}$ of L, and the same argument as in [5, p. 122] shows that this is identical to the usual "adjoint mapping" $X \rightarrow \mathrm{ad}(X)$ of $\mathfrak{w}$ into $\mathfrak{l}$, with $\mathrm{ad}(X) \cdot Y=[X,Y]$. As $\mathfrak{w}$ is simple, the kernel of the mapping $X \rightarrow \mathrm{ad}(X)$ is reduced to 0, hence, by the homomorphism theorem, the kernel N of $s \rightarrow \boldsymbol{f}_s$ is a finite normal subgroup of Γ; therefore, for $p \geqq 5$, Γ/N would be a solvable group. As G is isomorphic to $(\Gamma/N)^*$, G would be solvable, which is absurd.

NORTHWESTERN UNIVERSITY.

REFERENCES.

[1] A. Albert and M. S. Frank, "Simple Lie algebras of characteristic p," *Rend. Sem. Mat. Univ. e Polit. di Torino*, vol. 14 (1954-55), pp. 117-139.

[2] A. Borel, "Groupes linéaires algébriques," *Ann. of Math.*, vol. 64 (1956), pp. 20-82.

[3] N. Bourbaki, *Eléments de Mathématique*, Livre II, Algèbre, chap. I, *Actual. Scient. et Ind.*, no. 934-1144, Paris (Hermann), 1951.

[4] C. Chevalley, "On the theory of local rings," *Ann. of Math.*, vol. 44 (1943), pp. 690-708.

[5] ———, *Theory of Lie groups* I, Princeton University Press, 1946.

[6] ———, *Théorie des groupes de Lie*, Tome II, Groupes algébriques, *Actual. Scient. et Ind.*, no. 1152, Paris (Hermann), 1951.

[7] ———, Paper to be published on simple algebraic groups.

[8] J. Dieudonné, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$," *Comm. Math. Helv.*, vol. 28 (1954), pp. 87-118.

[9] ———, "Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$, (II)", *Amer. J. Math.*, vol. 77 (1955), pp. 218-244.

[10] ———, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$, (III)," *Math. Zeitsch.*, vol. 63 (1955), pp. 53-75.

[11] ———, "Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$, (IV)," *Amer. J. Math.*, vol. 77 (1955), pp. 429-452.

[12] ———, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$, (V)," *Bull. Soc. Math. France*, vol. 84 (1956), pp. 207-239.

[13] ———, "Sur la notion de variables canoniques," *Anais Acad. Bras. Ciencias*, vol. 27 (1955), pp. 251-258.

[14] N. Jacobson, "Abstract derivation and Lie algebras," *Trans. Amer. Math. Soc.*, vol. 42 (1937), pp. 216-217.

[15] ———, "Classes of restricted Lie algebras of characteristic p, II," *Duke Math. J.*, vol. 10 (1943), pp. 107-121.

[16] M. Rosenlicht, "Some basic theorems on algebraic groups," *Amer. J. Math.*, vol. 78 (1956), pp. 401-443.

[17] O. Zariski, "A simple analytical proof of a fundamental property of birational transformations," *Proc. Nat. Acad. Sci.*, vol. 35 (1949), pp. 62-66.

[18] I. Barsotti, "Structure theorems for group-varieties," *Ann. di Mat. pura ed appl.* (4), vol. 38 (1955), pp. 77-119.

ON MEAN MOTION.*

By RAOUF DOSS.

Introduction. Let $p(t)=\sum_1^N a_n \exp(i\lambda_n t)$ be a trigonometric polynomial. The Lagrange *mean motion* problem is to prove that the argument $\phi(t)$ of $p(t)$ has a mean value c, i.e., that there exists a limit

$$c=\lim[\phi(\delta)-\phi(\gamma)]/(\delta-\gamma) \text{ as } (\delta-\gamma)\to\infty.$$

The existence of the limit c has been stated in Jessen [4] and proved by Jessen and Tornehave in their paper [5]. We refer to this important paper for a full treatment of the Lagrange and allied problems and for bibliography.

Since $\arg p(t)$ is not determined at a zero of $p(t)$, we shall denote by $\arg^- p(t)$, viz. $\arg^+ p(t)$ any branch of $\arg p(t)$ which is continuous, except at a zero of $p(t)$, and discontinuous with a jump $-p\pi$ or $p\pi$ respectively when t is a zero of order p. In describing the t-axis this comes to avoid the zeros of $p(t)$ by means of small semi-circles in the negative or positive sense respectively. In a discontinuity point t_0 we define $\arg^- p(t_0)$ or $\arg^+ p(t_0)$ as the mean value of the limits from the two sides of t_0.

Put now $a^+(t)=\arg^+ p(t+1)-\arg^+ p(t)$, i.e., $a^+(t)$ is the variation of $\arg^+ p(t)$ along a segment of length 1; similarly define $a^-(t)$. Our main result (Theorem I) is that *the function* $a^+(t)$, (respectively $a^-(t)$), *is almost periodic in the sense of Riemann-Stepanoff.* (The R.S.a.p. functions form a subclass of the S.a.p. functions; see [3] or below).

As a consequence of this theorem we prove (Theorem II) that $\arg^+ p(t)$ *may be written in the form*

$$\arg^+ p(t)=ct+\int_0^t \alpha(u)\,du+\psi(t),$$

where c *is a constant,* $\alpha(t)$ *a Bohr a.p. function with mean-value zero and* $\psi(t)$ *a (bounded) R.S.a.p. function.* The first result of this type is due to Wintner [6].

It is useless to try to prove that the remainder $\arg^+ p(t)-ct$ is bounded. For, as shown by Bernstein [1], even in the case $N=3$, the remainder is generally unbounded.

---

* Received September 7, 1956; revised February 5, 1957.

In our proofs we use a deep result given by Jessen and Tornehave in [5]; but instead of applying the Kronecker-Weyl theorem (as Jessen and Torenhave) or the ergodic theorem (as Wintner) we use the theory of Riemann-Stepanoff a. p. functions.

We add that our theorems may be proved in a more general setting: $p(t)$ may be replaced by a function $f(s)$, almost periodic in a strip, having a finite integral base and an analytic *spatial extension.*

Notations and definitions. Let E be a measurable set and let its characteristic function be $c(x)$. We define the *S-measure* of E as

$$S(E) = \sup_{-\infty < x < \infty} \int_{x}^{x+1} c(u)\,du.$$

The complement of E with respect to the set R of all real numbers will be denoted by E^*.

A function $f(x)$ is said to be *almost periodic in the sense of Riemann-Stepanoff* (R. S. a. p.) if to every $\delta > 0$ there corresponds two trigonometric polynomials $p(x)$, $q(x)$ such that $p(x) \leqq f(x) \leqq q(x)$ and $D_S(p,q) < \delta$. Here $D_S(p,q)$ is the usual Stepanoff distance between the two functions $p(x)$, $q(x)$.

In order that the bounded function $f(x)$ be R. S. a. p. it is necessary and sufficient that to every $\delta > 0$ there corresponds a measurable set E and numbers $k > 0$, $\mu_1, \cdots, \mu_m$ such that $S(E^*) < \delta$, and such that $|f(x) - f(x')| < \delta$ provided $x \in E$ and provided that $|\mu_n x - \mu_n x'| < k$ $(\mathrm{mod}\, 2\pi)$, $(n = 1, \cdots, m)$. See [3].

Let the exponents $\lambda_1, \cdots, \lambda_N$ belong to the modul

$$M = \{h_1\mu_1 + \cdots + h_m\mu_m\}$$

where the numbers $\mu_1, \cdots, \mu_m$ are linearly independent and the set of coefficients $h_1, \cdots, h_m$ runs through all sets of integers. Denoting the inner product $h_1x_1 + \cdots + h_mx_m$ of two vectors $h = (h_n)$ and $x = (x_n)$ by hx, and allowing terms with the coefficient 0 we may write $p(t)$ in the form $p(t) = \sum a_h \exp(ih\mu t)$. The function $P(x) = \sum a_h \exp(ihx)$ is called the *spatial extension* of $p(t)$. Clearly $P(\mu t) = p(t)$. Spatial extension may also be defined for any almost periodic function $f(t)$ with a finite integral base $\mu_1, \cdots, \mu_m$.

Proofs of the theorems. We shall need the following lemmas:

LEMMA I. *Let $D(x_1, \cdots, x_m) = D(x_n)$ be a function of $x_1, \cdots, x_m$, of period 2π in each x_n, analytic in the domain $|x_n - x_n^0| \leqq 3h$, $(n = 1,$*

$\cdots, m$), and not identically zero. Let $\mu_1, \cdots, \mu_m$ be linearly independent numbers. Denote by $T(h)$ the set of points t at which $|\mu_n t - x_n^0| \leqq h$ $(\mathrm{mod}\, 2\pi)$, $(n = 1, \cdots, m)$. Then to every $\delta > 0$ we can associate an $\epsilon > 0$ such that the set $T(h, \epsilon)$ of the points $t \in T(h)$ at which $|D(\mu_n t)| < \epsilon$ has an S-measure less than δ.

Proof. Let $|y_n - x_n^0| < h$ $(\mathrm{mod}\, 2\pi)$, $(n = 1, \cdots, m)$. We first show that the function of θ, $D(\mu_n\theta + y_n)$, analytic in the domain $|\mu_n\theta| < 2h$ $(\mathrm{mod}\, 2\pi)$, $(n = 1, \cdots, m)$, does not vanish identically. In fact, due to the linear independence of the μ_n, the points $(\mu_n\theta + y_n)$ are everywhere dense, $\mathrm{mod}\, 2\pi$, in the set of points (x_n). Hence the set of points $(\mu_n\theta + y_n)$ for which $|\mu_n\theta + y_n - y_n| \leqq 2h$ $(\mathrm{mod}\, 2\pi)$, $(n = 1, \cdots, m)$ is everywhere dense, $\mathrm{mod}\, 2\pi$, in the set of points (x_n) for which $|x_n - y_n| < 2h$ $(n = 1, \cdots, m)$. Suppose therefore that the analytic function $D(\mu_n\theta + y_n)$ vanishes at every θ for which $|\mu_n\theta| \leqq 2h$ $(\mathrm{mod}\, 2\pi)$, $(n = 1, \cdots, m)$, then the function $D(x_n)$ vanishes at every point (x_n) at which $|x_n - y_n| < 2h$ $(n = 1, \cdots, m)$, and hence everywhere, against the hypothesis. Thus $D(\mu_n\theta + y_n)$ does not vanish identically.

Suppose now that the lemma is false. Then there exists a $\delta > 0$, a sequence of points t_r and a sequence of positive numbers $\epsilon_r \to 0$ such that, for the Lebesgue measure μ:

$$\mu\{T(h, \epsilon_r) \cap (t_r - \tfrac{1}{2}, t_r + \tfrac{1}{2})\} \geqq \delta.$$

Hence, choosing an arbitrary $\theta_r \in T(h, \epsilon_r) \cap (t_r - \frac{1}{2}, t_n + \frac{1}{2})$ we have

$$\mu\{T(h, \epsilon_r) \cap (\theta_r - 1, \theta_r + 1)\} \geqq \delta.$$

Let $t \in T(h, \epsilon_r) \cap (\theta_r - 1, \theta_r + 1)$. Put $\theta = t - \theta_r$. Since

$$(1) \qquad |\mu_n\theta_r - x_n^0| \leqq h \quad (\mathrm{mod}\, 2\pi), \qquad |\mu_n t - x_n^0| \leqq h \quad (\mathrm{mod}\, 2\pi), \quad (n = 1, \cdots, m),$$

then θ belongs to the domain Θ defined by the inequalities $|\theta| \leqq 1$ and $|\mu_n\theta| \leqq 2h$ $(\mathrm{mod}\, 2\pi)$, $(n = 1, \cdots, m)$. Moreover $|D(\mu_n\theta + \mu_n\theta_r)| < \epsilon_r$; Thus:

(2) the set of points $\theta \in \Theta$ for which $|D(\mu_n\theta + \mu_n\theta_r)| < \epsilon_r$ has a measure $\geqq \delta$.

Put

$$x_n^r = \mu_n\theta_r, \quad \mathrm{mod}\, 2\pi, \qquad 0 \leqq x_n^r < 2\pi, \quad (n = 1, \cdots, m),$$

and let $y = (y_n)$ be a limiting point of the (x_n^r). By (1), $|y_n - x_n^0| \leqq h$ $(\mathrm{mod}\, 2\pi)$, $(n = 1, \cdots, m)$. Now the function of θ, $D(\mu_n\theta + y_n)$ does not vanish identically. It is analytic in the domain Θ and this domain consists of a finite number of intervals. Hence, we can find an $\epsilon > 0$ such that

(2′) the set of points $\theta \in \Theta$ for which $|D(\mu_n\theta + y_n)| < \epsilon$ has a measure $< \delta$.

On the other hand, we can find an r such that $\epsilon_r < \epsilon/2$ and such that

$$|D(\mu_n\theta + \mu_n\theta_r) - D(\mu_n\theta + y_n)| < \epsilon/2,$$

for $\theta \in \Theta$. If $\theta \in \Theta$ is such that $|D(\mu_n\theta + \theta_r\mu_n)| < \epsilon_r$, then $|D(\mu_n\theta + y_n)| < \epsilon$, so that, by (2), the set of points $\theta \in \Theta$ at which $|D(\mu_n\theta + y_n) < \epsilon$ has a measure $\geqq \delta$: but this contradicts (2′), and the hypothesis that the lemma is false is untenable.

COROLLARY. *Let* $p(t) = \sum_1^N a_n \exp(i\lambda_n t)$ *be a trigonometric polynomial. Then, to every* $\delta > 0$ *we can associate an* $\epsilon > 0$ *such that the set of points* t *at which* $|p(t)| < \epsilon$ *has an* S*-measure* $< \delta$.

We just apply the lemma to the analytic spatial extension

$$P(x_n) = P(x) = \sum a_h \exp(ihx).$$

Remark. We shall use this corollary in the proof of Theorems I and II. To prove these theorems, not for a polynomial $p(t)$, but for a function $f(s)$, almost periodic in a strip and having a finite integral base and an analytic spatial extension, one should replace the corollary by the following statement whose direct proof presents no difficulty: "To every σ in the strip and to every $\delta > 0$ we can associate an $\epsilon > 0$ such that the set of points t at which $|f(\sigma + it)| < \epsilon$ has an S-measure less than δ."

THEOREM I. *Let* $p(t) = \sum_1^N a_n \exp(i\lambda_n t)$ *be a trigonometric polynomial. If* $a^+(t) = \arg^+ p(t+1) - \arg^+ p(t)$, *then* $a^+(t)$ *is an R.S.a.p. function.*

Proof. Using the notations above we put

$$P(x,t) = \sum a_h \exp(ihx) \exp(ih\mu t).$$

Denote by $a^+(x_n, 0)$ or $a^+(x, 0)$ the variation of $\arg^+ P(x,t)$ on the segment $(0,1)$ of the t-axis (so that $a^+(\mu_n t, 0) = a^+(t)$). Let $z(x,0)$ be the number of zeros of $P(x,t)$ on the same segment, a zero at an end point being counted with only half its multiplicity. We use the following result proved by Jessen and Tornehave ([5], p. 264):

"To every x^0 we can associate a neighbourhood $I(x^0, 3h^0)$: $|x_n - x_n^0| \leqq 3h^0$ $(n = 1, \cdots, m)$, and a finite number of functions not identically zero $D_1(x_1,\cdots,x_m)=D_1(x_n),\cdots,D_l(x_n)$, of period 2π in each x_n, analytic in the domain $I(x^0,3h^0)$ and such that $z(x,0)$ is a continuous function of x at every point $x\in I(x^0,3h^0)$ at which $D_1(x_n)\neq 0,\cdots,D_l(x_n)\neq 0$."

Replacing the functions $D_1(x_n),\cdots,D_l(x_n)$ by their product $D^0(x_n)$, we see that $z(x,0)$ is a continuous function of x at every point $x\in I(x^0,3h^0)$ at which $D^0(x_n)\neq 0$.

It is however obvious that for a point x at which $P(x,0)\neq 0$ and $P(x,1)\neq 0$ the continuity of $z(x,0)$ implies the continuity of $a^+(x,0)$.

The points x for which $0\leqq x_n\leqq 2\pi$ $(n=1,\cdots,m)$ form a compact set K. The covering of K by the sets $I(x^0,h^0)$ contains a finite covering, say, $I(x^0,h^0),\cdots,I(x^r,h^r)$. Let $\epsilon>0$ be arbitrary; let $I(x^j,h^j,\epsilon)$ be the set of points of $I(x^j,h^j)$ at which $D^j(x_n)|\geqq\epsilon$ and let P_ϵ be the set of x for which $|P(x,0)|\geqq\epsilon$, $|P(x,1)|\geqq\epsilon$. Then $a^+(x,0)$ is continuous at every point of the set

$$K_\epsilon=P_\epsilon\cap\bigcup_1^r I(x^j,h^j,\epsilon).$$

K_ϵ being compact, we prove in a standard manner that to every $\delta>0$ we can associate an $h=h_\delta$ such that $|a^+(x,0)-a^+(x',0)|<\delta$, provided $x\in K_\epsilon$ and provided $|x_n-x_n'|<h$ (mod 2π), $(n=1,\cdots,m)$.

We now go back to the variable t and put $x_n=\mu_nt$ (mod 2π) $0\leqq x_n\leqq 2\pi$, $(n=1,\cdots,m)$. Let T_ϵ be the set of points t for which $x\in K_\epsilon$. Then $|a^+(t)-a^+(t')|<\delta$, provided $t\in T_\epsilon$ and provided $|\mu_nt-\mu_nt'|<h$ (mod 2π), $(n=1,\cdots,m)$. Also the function $a^+(t)$ is bounded (see e.g., [5], p. 179).

To prove that $a^+(t)$ is an R. S. a. p. function there remains to show that we can find an $\epsilon>0$ for which $S(T_\epsilon^*)<\delta$.

Now if $t\in T_\epsilon^*$ then either $x\in P_\epsilon^*$ or for some $j=1,\cdots,r$, $x\in I(x^j,h^j)$, $x\notin I(x^j,h^j,\epsilon)$, i.e., t belongs to the set of points t for which $|D^j(\mu_nt)|<\epsilon$, and $|\mu_nt-x_n^j|<h^j$ (mod 2π), $(n=1,\cdots,m)$. By Lemma I, we can always choose $\epsilon>0$ such that each of these r sets has an S-measure less than $\delta/(r+1)$. By the Corollary, the set of points t for which $x\in P_\epsilon^*$ may also be given an S-measure less than $\delta/(r+1)$. This gives $S(T_\epsilon^*)<\delta$, and the theorem is proved.

Remark. In the same way we prove that for any $\delta>0$ the function $[\arg^+p(t+\delta)-\arg^+p(t)]$ is an R. S. a. p. function.

LEMMA II. *If $b(t)$ is an S. a. p. function and if $B(t)=\int_0^t b(u)du$ is bounded, then $B(t)$ is a Bohr a. p. function.*

The proof is identical with the classical proof of Bohr's theorem stating that if an indefinite integral of a Bohr a. p. function is bounded, then it is also a Bohr a. p. function (see e. g., [2], p. 7).

LEMMA III. *Let* $p(t)=\sum_1^N a_n \exp(i\lambda_n t)$ *be a trigonometric polynomial. Then there exists a Bohr a. p. function* $A(t)$ *such that*

$$\arg^+ p(t)=\int_0^t A(u)\,du+O(1).$$

Proof. We have

$$\int_0^n a^+(t)\,dt=\int_n^{n+1}\arg^+ p(t)\,dt-\int_0^1 \arg^+ p(t)\,dt=\arg^+ p(n)+O(1), \tag{3}$$

since the variation of $\arg^+ p(t)$ along any segment of length 1 is bounded. Put now

$$A(t)=\int_t^{t+1} a^+(u)\,du=\int_0^1 a^+(t+u)\,du.$$

Since $a^+(u)$ is an S. a. p. function then $A(t)$ is a Bohr a. p. function. But we have

$$\int_0^n A(t)\,dt=\int_0^n\int_0^1 a^+(t+u)\,du\,dt=\int_0^1\Big(\int_0^n a^+(t+u)\,dt\Big)du$$

$$=\int_0^1 \phi_n(u)\,du \quad (\text{say})=\phi_n(\theta) \qquad (0\leqq\theta\leqq 1)$$

$=\int_0^n a^+(\theta+t)\,dt=\int_\theta^{\theta+n} a^+(t)\,dt.$ Hence

$$\int_0^n A(t)\,dt-\int_0^n a^+(t)\,dt=\int_n^{n+\theta} a^+(t)\,dt-\int_0^\theta a^+(t)\,dt=O(1).$$

This gives, by (3), $\arg^+ p(n)=\int_0^n A(t)\,dt+O(1)$, and finally

$$\arg^+ p(t)=\int_0^t A(u)\,du+O(1).$$

THEOREM II. *Let* $p(t)=\sum_1^N a_n \exp(i\lambda_n t)$ *be a trigonometric polynomial. Then*

$$\arg^+ p(t)=ct+\int_0^t \alpha(u)\,du+\psi(t),$$

where c *is a constant,* $\alpha(t)$ *a Bohr a. p. function with mean value zero and* $\psi(t)$ *a (bounded) R. S. a. p. function.*

Proof. If c is the mean value of $A(t)$, then, by Lemma III, we can write

$$\arg^+ p(t) = ct + \int_0^t \alpha(u)\,du + \psi(t),$$

where $\alpha(t)$ is a Bohr a. p. function with mean-value zero and $\psi(t)$ is bounded. We shall prove that $\psi(t)$ is an R. S. a. p. function. Put

$$B(t) = \int_0^t \{\psi(u+1) - \psi(u)\}du = \int_t^{t+1} \psi(u+1)du - \int_0^1 \psi(u)du = O(1).$$

Since $\psi(t+1) - \psi(t)$ is an S. a. p. function, we see, by Lemma II, that $B(t)$ is a Bohr a. p. function, so that the function

$$\psi_1(t) = \int_t^{t+1} \psi(u)\,du$$

is also a Bohr a. p. function.

In the same way, using the fact that $\arg^+ p(t+\gamma) - \arg^+ p(t)$ is an R. S. a. p. function we prove that

$$\psi_\gamma(t) = \gamma^{-1} \int_t^{t+\gamma} \psi(u)\,du$$

is a Bohr a. p. function for any $\gamma > 0$.

Let now $\delta > 0$ be arbitrary. By the Corollary of Lemma I we can find an $\epsilon > 0$ such that, for the set $E_{2\epsilon}$ of points t at which $|p(t)| \geqq 2\epsilon$, we have

$$S(E_{2\epsilon}^*) < \delta. \tag{4}$$

Now ϵ being fixed, we can find an $h_0 > 0$ such that

$$|\arg^+ p(t+h) - \arg^+ p(t)| < \delta/6,$$

provided $t \in T_\epsilon$ and $|h| < h_0$. But

$$\psi(t+h) - \psi(t) = -ch - \int_t^{t+h} \alpha(u)du + \arg^+ p(t+h) - \arg^+ p(t).$$

Therefore we may find an $h_1 > 0$ such that $|\psi(t+h) - \psi(t)| < \delta/3$ for $t \in T_\epsilon$ and $|h| < h_1$. This shows that

$$|\psi_\gamma(t) - \psi(t)| < \delta/3 \tag{5}$$

for $t \in T_\epsilon$ and $|\gamma| < h_1$.

Take now a fixed positive $\gamma < h_1$. Since $\psi_\gamma(t)$ is a Bohr a. p. function we can find an $h_2 > 0$ and numbers $\nu_1, \cdots, \nu_m$, such that

$$|\psi_\gamma(t+\tau) - \psi_\gamma(t)| < \delta/3, \tag{6}$$

if only $|\nu_n\tau| < h_2 \pmod{2\pi}$ $(n = 1, \cdots, m')$. Also we can find an $h_3 > 0$ such that

$$(7) \qquad |p(t+\tau) - p(t)| < \epsilon,$$

provided that $|\mu_n\tau| < h_3 \pmod{2\pi}$, $(n = 1, \cdots, m)$. Now let $t \in E_{2\epsilon} \subset E_\epsilon$, and let

$$|\nu_n\tau| < h_2, \bmod 2\pi, \ (n = 1, \cdots, m'); \ |\mu_n\tau| < h_3, \bmod 2\pi, \ (n = 1, \cdots, m).$$

Then, by (7), $|p(t+\tau)| \geqq \epsilon$, so that $t + \tau \in T_\epsilon$. Therefore, by (5),

$$(8) \qquad |\psi(t+\tau) - \psi_\gamma(t+\tau)) < \delta/3.$$

Relations (8), (6) and (5) now give $|\psi(t+\tau) - \psi(t)| < \delta$. This shows, by (4), that $\psi(t)$ is an R. S. a. p. function and completes the proof of Theorem II.

CAIRO UNIVERSITY, EGYPT.

REFERENCES.

[1] F. Bernstein, "Über eine Anwendung der Mengenlehre auf ein aus der Theorie der säkularen Störungen herrührendes Problem," *Mathematische Annalen*, vol. 71 (1912), pp. 417-439.

[2] A. S. Besicovitch, *Almost Periodic Functions*, Cambridge, 1932.

[3] R. Doss, "On Riemann integrability and almost periodic functions," *Compositio Math.*, vol. 12 (1955), pp. 271-283.

[4] B. Jessen, "Sur un problème de Lagrange concernant l'argument d'un polynome trigonométrique," *C. R. Acad. Sci. Paris*, vol. 207 (1938), pp. 1081-1084.

[5] B. Jessen and H. Tornehave, "Mean motions and zeros of almost periodic functions," *Acta Mathematica*, vol. 77 (1945), pp. 137-279.

[6] A. Wintner, "On an ergodic analysis of the remainder term of mean motion," *Proceedings of the National Academy of Sciences*, vol. 26 (1940), pp 126-129.

ON DIFFERENTIAL EQUATIONS ON THE TORUS.*

By SHLOMO STERNBERG.

1. The study of differential equations on the torus was initiated by Poincaré in [3]. It was conjectured there, that for non-singular systems under suitable smoothness assumptions, either there exists a periodic solution or every solution path is dense on the torus. This result was first proved by Denjoy [1], cf. also Siegel [5]. More recently, it was shown by Saito [4] that if the flow generated by the differential equations is assumed to be measure preserving, then either every solution is periodic or the flow is ergodic, depending on the rationality or irrationality of a certain ratio. Thus all measure preserving flows on the torus behave qualitatively like a rectilinear flow on the Euclidean torus. We shall improve upon this result by showing that any flow on the torus with an invariant integral actually is rectilinear in the sense that by suitable choice of coordinates on the torus one can arrange that all the trajectories are straight lines. However the linearization of the time dependence depends intimately upon the arithmetical properties of the flow and becomes an issue of small divisors. It may be remarked that since Hamiltonian flows have an invariant integral, the following results are valid for a Hamiltonian system on the torus.[1]

2. We now state our principal theorem.

THEOREM 1. *Let the system of differential equations*

$$dx/dt = f(x,y), \qquad dy/dt = g(x,y) \tag{1}$$

be of class C^n and defined on the torus, i. e. let f and g be periodic of period one in both variables. Furthermore assume that the differential equations (1) *possess an integral invariant $U(x,y)$ of class C^n defined on the torus. Then there exists a change of coordinates*

$$X = X(x,y), \qquad Y = Y(x,y) \tag{2}$$

---

* Received October 4, 1956.

[1] The results of this paper were obtained during participation in a seminar conducted by Professor Wintner.

such that in the new coordinate system the differential equations (1) *have the form*

$$(3) \qquad dX/dt = F(X,Y), \qquad dY/dt = \gamma F(X,y).$$

Thus in these new coordinates the trajectories are all straight lines.

In the proof of this theorem, essential use will be made of the nonbounding cycle without contact introduced by Siegel in [5]. We remark that in the present case, this cycle can be chosen to be of class C^{n+1}. This follows immediately from Siegel's construction. In fact, the cycle without contact is constructed by considering the orthogonal trajectories to (1). If the orthogonal system has a periodic solution, this provides the desired cycle. It is clearly of class C^{n+1} since the differential equations are of class C^n. In the complementary case one closes up an orthogonal trajectory in the neighborhood of a limit point where the vector field is approximately constant; and this can be done in a smooth manner. For the details the reader is referred to [5].

3. Let Γ be the cycle without contact. We wish to construct a family of such cycles filling up the torus. The natural thing to do, would be to allow the points of Γ to follow the flow generated by the differential equations. However, this procedure, as it stands, would lead to difficulties since the points flow with different speeds along different trajectories, thus leading to the situation where one point on Γ will have returned to Γ at a given time, whereas another point might not have. This difficulty can be avoided simply by speeding up the flow on the slow trajectories and slowing down the flow on the fast ones: if we denote by $t(s)$ the length of time it takes for a point on the cycle (parametrized by s) to return to Γ under the flow, then $t(s)$ is a function of class C^{n+1}. Denote by $\Gamma(s;\tau)$ the image of the point $\Gamma(s)$ under the flow corresponding to the time $t = t(s) \cdot \tau$. The family of curves $\Gamma(\cdot\,;\tau)$ provides us with the desired family of cycles without contact. We can now introduce the function $\tau(x,y)$ which tells what cycle $\Gamma(\cdot\,;\tau)$ the point (x,y) is on. This function essentially tells us how far the point (x,y) is along a trajectory; we now wish to introduce a parameter which tells us which trajectory the point (x,y) is on. For this purpose we make use of the integral invariant. Now the fact that U is an integral invariant can be expressed analytically as

$$(4) \qquad (Uf)_x + (Ug)_y = 0.$$

This, in turn, implies the existence of a function $H(x,y)$ satisfying

$$H_y = Uf, \qquad H_x = -Ug. \tag{5}$$

Thus

$$dH/dt = H_x f + H_y g = 0: \tag{6}$$

i.e., H is an integral of the flow. The function H is not defined on the torus but in the plane, i.e., it is not necessarily periodic. However, by virtue of (5), the partial derivatives of H are periodic and we may write

$$H(x,y) = ax + by + h(x,y), \tag{7}$$

where h is a function of class C^{n+1} on the torus. Since the system (1) is non-singular, the function H cannot assume the same value for two distinct trajectories in the plane. We now set

$$X = \tau(x,y), \qquad Y = \alpha\tau(x,y) + \beta H(x,y), \tag{8}$$

where α and β are chosen so that

$$\begin{aligned} &\alpha(\tau(x,y) - \tau(x+1,y)) + \beta(H(x,y) - H(x+1,y) = m, \\ &\alpha(\tau(x,y) - \tau(x,y+1)) + \beta(H(x,y) - H(x,y+1) = n, \end{aligned} \tag{9}$$

where m and n are integers. It is clear that the change of coordinates (8) transforms (1) to the form (3) with $\gamma = \alpha$.

4. In order to obtain an explicit formula for γ we first show that by proper linear area preserving changes of coordinates we can arrange that the cycles without contact are homotopic to the cycle $x = 0$. This is a well known result that we include here for completeness.

LEMMA 1. *Let K be a non-bounding non-self-intersecting cycle defined on the torus T. Then there exists a linear area preserving homeomorphism of T onto a torus T' such that image K' of K is homotopic to the cyclic $x = 0$.*[2]

It is clear from the structure of the fundamental group of the torus that we can find a linear automorphism of the torus of the form $x' = ax + by$, $y' = cx + dy$ with integral a, b, c, d and $ad - bc = \pm 1$ and is therefore area preserving such that K is homotopic to some multiple m of the cycle $x = 0$. We now show that $m = 1$. In fact, let $\boldsymbol{K}$ denote the curve in the plane which covers K. If $m = \pm 1$ then the translate of $\boldsymbol{K}$ by the vector

---

[2] The following proof of the lemma was obtained jointly with Harry Furstenberg.

$(0,1)$ does not intersect $\boldsymbol{K}$ and so must lie entirely in one of the two domains in the plane bounded by $\boldsymbol{K}$. Repeating this procedure m times leads to a contradiction.

In these new coordinates the function τ satisfies the equations

$$\tau(x+1,y)-\tau(x,y)=1, \qquad \tau(x,y+1)-\tau(x,y)=0;$$

we may thus choose α and β in (10) as $-a/b$ and $1/b$ respectively. Here it is to be remarked that a, b, f and g are all to be calculated in the new coordinate system (and that f and g transform as vectors).

By (5) and (7) we have

$$(10) \qquad a=H(x+1,y)-H(x,y)=\int_0^1 H_x(x,y)\,dx$$
$$=\int_0^1\int_0^1 H_x(x,y)\,dxdy=-\iint_T Ugdxdy.$$

Similarly,

$$(11) \qquad b=\iint_T Ufdxdy.$$

Combining (10), (11) and (9), we obtain

$$(12) \qquad \gamma=\iint_T Ufdxdy/\iint_T Ugdxdy.$$

This formula was obtained in the new coordinate system. However since both sides of (12) transform in the same manner under linear change of coordinates, (12) holds in the original coordinate system.

5. The results of paragraph 2 may be summed up by saying that given any system (2) with a smooth invariant measure, we can find a smooth change of coordinates which makes all the trajectories of (2) linear. In these new coordinates the dependence on the time, is still, however, non-linear. The question of whether or not we can linearize the time dependence, depends on the arithmetic nature of the invariant τ. The following result is due to Kolmorgoroff [2]. It is essentially equivalent to a previous result of Wintner [6].

THEOREM. *Let $F(X,Y)$ be an analytic function on the torus. A sufficient condition for the existence of an analytic change of coordinates sending the system* (3) *into the system*

$$(13) \qquad dx/dt=A, \qquad dy/dt=B; \qquad A/B=\gamma.$$

is that there exists two constants $K > 0$ and $h > 0$, such that for all integers m and n,

(14) $$|m - n\gamma| > Kh^{n}.$$

Remark. If condition (14) is not satisfied, then there exists a γ and an F such that (3) can be transformed into the form (13) by a change of coordinates which is of class C^{∞} or of class C^{k} but not C^{k+1} for any k.

It is clear that any two coordinate systems in which (3) has the form (14) can differ only by a linear transformation, so that as far as smoothness considerations are concerned, the change of coordinates is essentially unique. Now if we were operating in the plane, the change of coordinates

$$x^{*} = kT(X,Y) = k\int_{0}^{X}(1/F(z, Y + \gamma(z - x)))dz,$$

$$y^{*} = Y + \gamma(x^{*} - X),$$

would have the desired effect. In fact all we have to check is dx^{*}/dt. But

$$\partial x^{*}/\partial X = k(1/F(X,Y)) + k\int_{0}^{X}(1/F)_{Y}dz\cdot(-\gamma), \quad \partial x^{*}/\partial Y = k\int_{0}^{X}(1/F)_{Y}dz,$$

so that $dx^{*}/dt = F(X,Y)\partial x^{*}/\partial X + \gamma F(X,Y)\partial x^{*}/\partial Y = k$.

We now have to modify x^{*} so that it becomes periodic. We may do this without affecting the form (13) by adding a suitable function of $Y + \gamma X$. Setting $G = 1/F$ we have (since G is periodic),

$$T(X+1,Y) = \int_{0}^{X+1} G(z, Y + \gamma(z - X))dz = \int_{-1}^{X} G(z, Y - \gamma X + \gamma(z - 1))ds.$$

Thus $T(X+1,Y) - T(X,Y) = \int_{0}^{1} G(s, Y + \gamma(s - X))ds - S(Y - \gamma X)$, where

$$S(Z) = \int_{0}^{1} G(z, Z + \gamma(s - 1))dz = T(1, Z).$$

Setting $1/k = \int_{0}^{1} S(Z)dZ = \int_{0}^{1}\int_{0}^{1}(1/F)dxdy$, we see that if $R(Z)$ is a solution of the functional equation

(15) $$R(s + \gamma) - R(s) = S(s) - 1/k,$$

then the change of coordinates

(16) $$x = k(T(X,Y) + R(Y - X)), \qquad y = Y + \gamma(x - X),$$

has the desired properties. But (15) is a difference equation in angular variables so that the results of [6] are applicable.

Expanding S into a Fourier series

$$S(w) = 1/k + \sum_{n \neq 0} a_n e^{2\pi i n w},$$

equation (15) has the formal solution

$$R(w) = \sum_{n \neq 0} a_n e^{2\pi i n w} / (e^{2\pi i n \gamma} - 1).$$

Since $S(w)$ is analytic, condition (14) assures the analyticity of R. As we can choose S arbitrarily by proper choice of F, this proves the remark following the theorem.

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] A. Denjoy, "Sur les courbes définies par les équations différentielles a la surface de la tore," *Journal de Mathématiques Pures et Appliquées*, ser. 9, vol. 11 (1932), pp. 333-375.

[2] A. Kolmogoroff, *Doklady*, vol. 93 (1953), pp. 763-766.

[3] H. Poincaré, "Sur les courbes définies par les équations différentielles," *Œuvres*, vol. 1, pp. 137-158.

[4] T. Saito, "On the measure preserving flow on the torus," *Journal of the Mathematical Society of Japan*, vol. 3 (1951), pp. 279-284.

[5] C. L. Siegel, "On differential equations on the torus," *Annals of Mathematics*, vol. 46 (1945), pp. 423-428.

[6] A. Wintner, "The linear difference equation of first order for angular valuables," *Duke Mathematical Journal*, vol. 12 (1945), pp. 445-449.

2. DeRham's theorem and Dolbeault's theorem. We let $\mathfrak{V}$ be a C^∞ V-manifold. If B is a V-bundle over $\mathfrak{V}$ with a vector space as fibre, it is clear that the sections of B over an open subset $\mathfrak{O}$ of $\mathfrak{V}$ form an additive group. We let A^p denote the bundle of differential p-forms for $\mathfrak{V}$ and let $\mathfrak{J}^p$ denote the sheaf of germs of C^∞ sections of A^p. It is clear that $\mathfrak{J}^p$ is a fine sheaf, since there exists a C^∞ partition of unity subordinate to any locally finite covering of $\mathfrak{V}$, and therefore (see [21]) $H^q(\mathfrak{V}, \mathfrak{J}^p) = 0$ if $q \geqq 1$, while, as always, $H^0(\mathfrak{V}, \mathfrak{J}^p) = \mathfrak{M}^p$ is the module of C^∞ sections of A^p. We let D^p denote the subsheaf of $\mathfrak{J}^p$ consisting of germs of forms ϕ such that $d\phi = 0$ (i.e., such that ϕ is closed). Then since $d^2 = 0$, d induces a homomorphism, also denoted by d, of $\mathfrak{J}^p$ into D^{p+1}. We now show that d maps $\mathfrak{J}^p$ onto D^{p+1}. Let $x \in \mathfrak{V}$, let ϕ be a closed C^∞ differential $(p+1)$-form (i.e., a C^∞ section of A^{p+1}) in a neighborhood W of x and let $\{U, G, v\}$ [2] be a l.u.s. for $\mathfrak{V}$ such that $x \in \bar{U} \subset W$. Then in U, ϕ is represented by a C^∞ G-invariant differential $(p+1)$-form ϕ_U such that $d\phi_U = 0$. Let $y \in v^{-1}(x)$. By the Poincaré lemma there exists a C^∞ differential p-form ψ in a small neighborhood N of y such that $d\psi = \phi_U$, and we may assume that $gN \cap N$ is empty unless g belongs to the subgroup G_y of G leaving y fixed, while $gN = N$ if $g \in G_y$. We put $\psi_N{}^* = (1/\operatorname{ord} G_y) \sum_{g \in G_y} \psi_g$, where $\psi_g(\eta) = g^*\psi(g\eta)$, $\eta \in N$, and g^* is the mapping of differential forms dual to g. Then since d commutes with the mapping of differential forms dual to a differentiable mapping of one manifold into another, it follows that $d\psi_N{}^* = \phi_U$. Since $\psi_N{}^*$ is invariant under G_y, $\psi_N{}^*$ induces a C^∞ differential p-form ψ^* in a small neighborhood of x on $\mathfrak{V}$ such that $d\psi^* = \phi$. Hence $d: \mathfrak{J}^p \to D^{p+1}$ is onto. Therefore the sequence of sheaves

$$0 \to D^p \to \mathfrak{J}^p \to D^{p+1} \to 0$$

is exact. From the associated exact cohomology sequence we obtain by a well-known inductive process, using the fact that $H^q(\mathfrak{V}, \mathfrak{J}^p) = 0$ if $q \geqq 1$, that $H^q(\mathfrak{V}, D^0) \cong \mathfrak{Z}^q / d\mathfrak{M}^{q-1}$, $q \geqq 1$, where $\mathfrak{Z}$ is the module of C^∞ closed forms of degree q, and since D^0 is just the constant sheaf of real numbers, $H^q(\mathfrak{V}, R) \cong \mathfrak{Z}^q / d\mathfrak{M}^{q-1}$; thus we have obtained another proof (see Satake [17]) of de Rham's theorem which is analogous to that given by Weil for C^∞ manifolds [24]. Let $\mathfrak{V}$ be supplied with a Riemann metric. Coupling the above result with Theorem H of [2] we have $H^q(\mathfrak{V}, R) = \mathfrak{H}^q$, where $\mathfrak{H}^q$ is the finite dimensional module of real harmonic differential forms of degree q on $\mathfrak{V}$.

---

[2] In this paper we denote a l.u.s. by $\{U, G, v\}$ instead of by $\{U, G, \phi\}$ as in [2]. Furthermore, ∂ and $\bar{\partial}$ of [2] have been replaced by d' and d'' respectively.

Now let $\mathfrak{V}$ be a compact, complex analytic V-manifold and let B be a complex line bundle over $\mathfrak{V}$. We let $A^{r,s}$ denote the bundle of forms of type (r,s) on $\mathfrak{V}$. Then we denote by $\mathfrak{F}^{r,s}(B)$ the sheaf of germs of C^∞ sections of $B\otimes A^{r,s}$. It is clear that $\mathfrak{F}^{r,s}(B)$ is a fine sheaf so that $H^q(\mathfrak{V},\mathfrak{F}^{r,s}(B))=0$ if $q\geqq 1$, while, if $\mathfrak{M}(B)^{r,s}$ is the module of C^∞ forms of type (r,s) with coefficients in B, $H^0(\mathfrak{V},\mathfrak{F}^{r,s}(B))=\mathfrak{M}(B)^{r,s}$. We let $D^{r,s}(B)$ denote the subsheaf of $\mathfrak{F}^{r,s}(B)$ consisting of germs of C^∞ sections ϕ of $B\otimes A^{r,s}$ such that $d''\phi=0$. Since $d''^2=0$, it follows that d'' induces a homomorphism of $\mathfrak{F}^{r,s}(B)$ into $D^{r,s+1}(B)$. We may then use Dolbeault's lemma (see [11]) in the same role as we previously used Poincaré's lemma, together with the fact that d'' commutes with complex analytic mappings and multiplication by a holomorphic function, to prove, by use of an obvious local averaging process, that $d''\colon\mathfrak{F}^{r,s}(B)\to D^{r,s+1}(B)$ is onto. Therefore the sequence of sheaves

$$0\to D^{r,s}(B)\to\mathfrak{F}^{r,s}(B)\to D^{r,s+1}(B)\to 0$$

is exact. From the associated exact cohomology sequence we again obtain, by an inductive process, that

$$H^s(\mathfrak{V},D^{r,0}(B))=\mathfrak{Z}^{r,s}(B)/d''\mathfrak{M}^{r,s-1}(B),\quad s\geqq 1,$$

where $\mathfrak{Z}^{r,s}(B)$ is the module of d''-closed forms of type (r,s) with coefficients in B; and since $D^{r,0}(B)$ is just the sheaf of germs of holomorphic r-forms with coefficients in B, which we denote by $\Omega^r(B)$, we obtain

$$H^s(\mathfrak{V},\Omega^r(B))=\mathfrak{Z}^{r,s}(B)/d''\mathfrak{M}^{r,s-1}(B),\quad s\geqq 1,$$

which is Dolbeault's theorem. If $\mathfrak{V}$ is supplied with a Hermitian metric and B is supplied with a C^∞ metric, we may couple the above result with Theorem K of [2] to obtain

THEOREM D-K. $H^s(\mathfrak{V},\Omega^r(B))=\mathcal{H}(B)^{r,s}$,

which we will refer to as Dolbeault-Kodaira's theorem.

3. Certain definitions for V-manifolds.

Let $\mathfrak{V}$ be a compact C^∞ V-manifold. Let $\{U,G,v\}$ be a l.u.s. for $\mathfrak{V}$, let $x\in U$, and let G_x be the subgroup of G leaving x fixed. We say that $x^*=v(x)\in\tilde{U}$ is a regular point on $\mathfrak{V}$ if G_x consists of the identity alone; otherwise we say that x^* is singular. We let $m_x=\operatorname{ord}G_x$ and call m_x the order of x. We define $m_0=\mathrm{l.c.m.}_{x^*\in\mathfrak{V}}\,m_x$ and call m_0 the order of $\mathfrak{V}$; clearly m_0 is finite since $\mathfrak{V}$ is compact. It is evident that the above definitions do not depend on the choice of l. u. s. The regular points of $\mathfrak{V}$ form a C^∞ manifold in the ordinary sense. From our definition in [2], it is clear that we may naturally identify the ring of germs of C^∞ functions at x^* on $\mathfrak{V}$ with the ring of germs of G-invariant C^∞ functions on U at x. If $\mathfrak{V}$ is a complex analytic V-manifold, it follows from a known theorem on removable singularities that the ring of germs of holomorphic functions at x^*, in addition to being naturally identified with the ring of germs of G-invariant holomorphic functions at x, also coincides with the ring of germs of continuous functions at x^* which are holomorphic at all the regular points of $\mathfrak{V}$ in a neighborhood of x.

We now let $\mathfrak{V}$ be a compact, complex analytic V-manifold. By a known theorem [6], we will assume, without loss of generality, that for each l. u. s. $\{U, G, v\}$ G acts as a finite linear group in the coordinates of U. By a divisor over $\mathfrak{V}$ we mean that, for each l. u. s. $\{U, G, v\}$, we are given a divisor $\boldsymbol{D}_U$ on U such that, if f belongs to the module $\boldsymbol{D}_U(gx)$ over the ring $\mathfrak{O}_{gx}$ of local holomorphic functions at $gx \in U$ which are locally multiples of $\boldsymbol{D}_U$, then $f \circ g$ belongs to $\boldsymbol{D}_U(x)$ for each $x \in U$, $g \in G$, and such that, if λ is an injection of $\{U', G', v'\}$ into $\{U, G, v\}$ and if f belongs to $\boldsymbol{D}_U(\lambda(y))$ at $\lambda(y) \in \lambda(U')$, then $f \circ \lambda$ belongs to $\boldsymbol{D}_{U'}(y)$. We say that $\boldsymbol{D}$ is an absolute divisor (i. e., locally linearly equivalent to zero) on $\mathfrak{V}$ if at each $x \in \mathfrak{V}$ there exists a l. u. s. $\{U, G, v\}$, $x \in \tilde{U}$, such that $\boldsymbol{D}_U$ is the divisor (f_U) of a single meromorphic function f_U in U which can be expressed as the quotient of two relatively prime G-invariant holomorphic functions. It is not necessarily true that a divisor $\boldsymbol{D}$ over $\mathfrak{V}$ is an absolute divisor, but if m_0 is the degree of $\mathfrak{V}$, then $m_0\boldsymbol{D}$ is absolute. To see this, we let $x \in \mathfrak{V}$, let $\{U, G, v\}$ be a l. u. s., $x \in \tilde{U}$, such that $\boldsymbol{D}_U$ is the divisor (f_U) of a quotient of two holomorphic functions, and let $m = \operatorname{ord} G$; f_U is not necessarily the quotient of two relatively prime, G-invariant, holomorphic functions, but, the product $\boldsymbol{p}_U$ of its tranlates under G clearly is, and $(\boldsymbol{p}_U{}^{(m_0/m)}) = m_0\boldsymbol{D}_U$ in view of the invariance of $\boldsymbol{D}_U$ *under* G. (In this connection see [20], exposé XX.)

Let B be a V-bundle over $\mathfrak{V}$ (see [2]). We may assume without loss of generality that B_U is the product bundle for each l. u. s. $\{U, G, v\}$. Then if $g \in G$ and $(z, \zeta) \in B_U$, $h_U(g)(z, \zeta) = (g^{-1}z, \eta_U(g)(z) \cdot \zeta)$, while if λ is an injection of $\{U, G, v\}$ into $\{U', G', v'\}$, $z \in U$, and $(\lambda(z), \zeta) \in B_{U'} \mid \lambda(U)$, then $\lambda^*(\lambda(z), \zeta) = (z, \xi_\lambda(\lambda(z)) \cdot \zeta)$, where $\eta_U(g)$ and ξ_λ are, respectively, mappings of U and $\lambda(U)$ into the group of the bundle; in particular, if B is a complex line bundle, $\eta_U(g)$ *and* ξ_λ are non-zero holomorphic functions. It is clear, from the definition of V-bundle, that $\eta_U(g_2)(g_1{}^{-1}z)\eta_U(g_1)(z) = \eta_U(g_1g_2)(z)$ and $\eta_U(g)(z)\xi_\lambda(\lambda(z)) = \xi_\lambda(\lambda(g^{-1}z))\eta_{U'}(g')(\lambda(z))$, where $g, g_1, g_2 \in G$ and $z \in U$, while if λ' is an injection of $\{U', G', v'\}$ into $\{U'', G'', v''\}$, then $\xi_\lambda(\lambda(z))\xi_{\lambda'}(\lambda'\lambda(z))=\xi_{\lambda'\lambda}(\lambda'\lambda(z))$. Conversely, if $\{\eta_U(g)\}$ and $\{\xi_\lambda\}$ are given subject to these conditions, it is clear that we obtain a V-bundle in a natural manner. We say that two V-bundles B_1 and B_2 having a given differentiable structure are equivalent if, for each l. u. s. $\{U, G, v\}$, there exists a map θ_U of U into the group of the bundle such that

(1) θ_U belongs to the same class of differentiability as the bundles B_1 and B_2.

(2) If $g \in G$ and $z \in U$, then

$$\eta^1{}_U(g)(z)\theta_U(z)=\theta_U(g^{-1}z)\eta^2{}_U(g)(z)$$

and

$$\xi^1{}_\lambda(\lambda(z))\theta_{U'}(\lambda(z))=\theta_U(z)\xi^2{}_\lambda(\lambda(z)),$$

where $\eta^1{}_U$, $\xi^1{}_\lambda$ and $\eta^2{}_U(g)$, $\xi^2{}_\lambda$ are corresponding functions for B_1 and B_2 respectively.

Now suppose that B is a V-bundle, the group of which is some linear group. We say that B is an absolute V-bundle if, in addition to the requirements stipulated in [2], the following condition is satisfied: If $\{U, G, v\}$ is a l. u. s. and $g \in G_x$, then $h_U(g)b=b$ for each b in the fibre of B_U over x. We can give a useful characterization of absolute bundles (up to equivalence). Let B be an absolute V-bundle. Let $\{U, G, v\}$ be a l. u. s. and define $\theta_U(z)=(\operatorname{ord} G)^{-1}\sum_{g\in G}\eta_U(g)(z)$. Since B is an absolute V-bundle, $\eta_U(g)(z)$ is the identity if $gz=z$, and therefore if $y \in U$ and $G_y=G$, θ_U defines a mapping of a small neighborhood of y into the group of the bundle. By choosing a sufficiently small l. u. s. $\{U, G, v\}$, we may assume that θ_U is defined in all of U. It is easily seen that, for $g \in G$, $\theta_U(g^{-1}z)\eta_U(g)(z)=\theta_U(z)$. Therefore, if we define $\xi^*{}_\lambda(\lambda(z))=\theta_U(z)\xi_\lambda(\lambda(z))\theta_{U'}(z))^{-1}$, it is clear that $\xi^*{}_\lambda(\lambda(gz))=\xi^*{}_\lambda(\lambda(z))$. Hence the system of functions $\xi^*{}_\lambda$ and $\eta_U(g)^*$, defined by $\eta_U(g)^*=$ identity, define a V-bundle B^* equivalent to B. Hence, up to equivalence, *an absolute V-bundle B may be naturally regarded as a bundle over $\mathfrak{V}$ itself whose coordinate transformations are given by functions of a certain differentiability class on intersections of neighborhoods for B on $\mathfrak{V}$.*

Let B be a complex line bundle over $\mathfrak{V}$ and let a be a C^∞ metric for B. Then for each l. u. s. a_U is a C^∞ positive, real-valued function, and it is clear (using m(i), section 2 of [2]) that the differential form $\phi_U=\frac{i}{2\pi}d'd''\log a_U{}^{-1}$ is G-invariant in U and that the collection of differential forms $\{\phi_U\}$ defines a closed differential form ϕ on $\mathfrak{V}$. By Section 2, ϕ defines a certain 2-dimensional cohomology class on $\mathfrak{V}$, which we call the characteristic class of B. It is not hard to see that this cohomology class is independent of the choice of metric. Moreover, ϕ is Hermitian, and if ϕ is positive definite, $\phi > 0$, ϕ provides a Kähler metric for $\mathcal{V}$; in this case ϕ is called a Hodge metric, and B is said to be positive (or ample), $B > 0$, if a metric a can be found such that ϕ is positive. Our principal result, stated more precisely in the very last section, is that, if there exists a positive complex line bundle over the compact, complex analytic V-manifold $\mathcal{V}$, then $\mathcal{V}$ is an algebraic variety.

Equivalence classes of complex line bundles over $\mathcal{V}$ form an additive group in an evident manner (see [16]).

If $\boldsymbol{D}$ is a divisor on $\mathcal{V}$, $\boldsymbol{D}$ naturally defines a complex line bundle $\{\boldsymbol{D}\}$ over $\mathcal{V}$. Namely, if $\{\{U, G, v\}\}$ is a collection of l. u. s.'s such that $\{\tilde{U}\}$ is a base of neighborhoods for $\mathcal{V}$, and if $\boldsymbol{D}_U$ is the divisor of the function f_U in each U, we define $\eta_U(g)(z) = (f_U \circ g^{-1})(z)/f_U(z)$, $g \in G$, and if $\lambda : U \rightarrow U'$ is an injection, we define $\xi_\lambda(\lambda(z)) = f_U(z)/(f_{U'} \circ \lambda)(z)$. It is clear that $\eta_U(g)$ and ξ_λ are non-zero holomorphic functions and satisfy the necessary conditions for defining a bundle. In particular, if $\boldsymbol{D}$ is an absolute divisor, we may assume each f_U is G-invariant so that each $\eta_U(g) = 1$ in U and therefore $\{\boldsymbol{D}\}$ is an absolute bundle. The characteristic class of $\{\boldsymbol{D}\}$ is also called the characteristic class of $\boldsymbol{D}$. Another motivation for the given definition of an absolute divisor is that it may be viewed locally as a divisor over the ring of local holomorphic functions at a point on $\mathcal{V}$. Just as it was shown for any divisor $\boldsymbol{D}$ over $\mathcal{V}$ that $m_0\boldsymbol{D}$ is an absolute divisor, where m_0 is the degree $\mathcal{V}$, so it can be shown for any complex line bundle B over $\mathcal{V}$ that m_0B is absolute. In fact, if $\{U, G, v\}$ is a l. u. s. and η_U is the corresponding function defined for B, then $\eta_U(g)(z)$ is an m_0-th root of unity whenever $gz = z$, $g \in G$, $z \in U$. These facts correspond roughly to the fact that if K is an algebraic extension of the field k, then the norm of an ideal in K is an ideal in k. In fact, in many cases of interest the divisors over $\mathcal{V}$ appear as divisors invariant under the fundamental group of a kind of universal covering space of $\mathcal{V}$.

Let f: $z \rightarrow f(z)$ be a complex analytic mapping, with non-vanishing Jacobian, from an open set $\mathcal{O}$ in C^n into C^n, let the coordinates of $f(z)$ be $f^1(z), \cdot\cdot, f^n(z)$, and let the coordinates in $\mathcal{O}$ be $z^1, \cdot\cdot\cdot, z^n$. Then we write

$$J(f)(p) = [\det(\partial f^i/\partial z^j)]_p^{-1}, \quad p \in \mathcal{O}.$$

We define the *canonical bundle* K over $\mathcal{V}$ to be the complex line bundle over $\mathcal{V}$ for which the functions η_U and ξ_λ are defined as follows:

$$\eta_U(g)(z) = J(g^{-1})(z)$$

and

$$\xi_\lambda(\lambda(z)) = J(\lambda^{-1})(\lambda(z)).$$

Let γ be a Hermitian metric for $\mathcal{V}$. Then for each l. u. s. $\{U, G, v\}$, γ is a positive definite Hermitian matrix function $(\gamma_{U\alpha\beta'})$[3] and direct calculation shows that the system of functions $a_U = (\det(\gamma_{U\alpha\beta'}))^{-1}$ defines a metric a for the bundle K; hence the collection of forms

$$\phi_U = \frac{i}{2\pi}\, d'd'' \log(\det(\gamma_{U\alpha\beta'}))$$

defines a closed form ϕ in the characteristic class of K. The form R of type $(1,1)$, defined by $\frac{i}{2\pi} R = \phi$, we call the Ricci curvature of the metric γ. For a given l. u. s. $\{U, G, v\}$

$$R_U = \Sigma R_{U\lambda\mu'} dz^\lambda d\bar{z}^\mu = d'd'' \log(\det(\gamma_{U\alpha\beta'})).$$

In the future we will have use for the tensor R^* defined in U by

$$R^*{}_U{}^{\mu'}{}_{\alpha'} = \Sigma \gamma_U{}^{\lambda\mu'} R_{U\lambda\alpha'},$$

where $(\gamma_U{}^{\lambda\mu'})$ is the matrix inverse of $(\gamma_{U\alpha\beta'})$.

Let X be a C^∞ manifold and let C be a discontinuous group of C^∞ homeomorphisms of X satisfying the following conditions:

(1) If $x, y \in X$ and $y \notin Gx$, there exist neighborhoods U of x and V of y such that $GU \cap GV$ is empty.

(2) X/G is compact.

(3) If $x \in X$, the subgroup G_x of G leaving x fixed is finite.

(4) Each point $x \in X$ has a neighborhood U such that $gU \cap U$ is empty if $g \notin G_x$.

Then is it clear that X/G is a V-manifold. If we replace C^∞ by "complex analytic," X/G is a complex analytic V-manifold. It is clear that we obtain a V-bundle B over X/G in a natural way if we let B^* be a bundle over X and prescribe an anti-isomorphism h of G into a group of bundle maps of B^* onto itself such that if $g \in G$, $x \in X$, then $h(g)$ carries the fibre over x onto the fibre over $g^{-1}x$. The modifications of these statements for the C^∞ and complex analytic cases are obvious, as is also the necessary and sufficient condition under which the bundle induced over X/G is absolute There is an obvious correspondence between the sections of B and the cross-sections of B^* invariant under $h(G)$. An important special case is obtained by letting X be a bounded domain $\mathfrak{D}$ in C^n and G a properly discontinuous group of complex analytic automorphisms of $\mathfrak{D}$. We let B^* be the product bundle $\mathfrak{D} \times C$ and define $h(g)(z,\zeta) = (g^{-1}z, J(g^{-1})(z)\cdot\zeta)$. Then a metric for B^* invariant under $h(g)$ is given by $\mathfrak{K}^{-1}$, where $\mathfrak{K}$ is the kernel function (see [3]), and since $d'd'' \log \mathfrak{K}$ is the G-invariant (positive definite) Bergman metric, we see that the complex line bundle B over $\mathfrak{D}/G$ induced by B^* and h is positive. Hence it will be an immediate consequence of our main result that $\mathfrak{D}/G$ is an algebraic variety. It is easily seen that B is simply the canonical bundle K for $\mathfrak{D}/G$.

---

[3] Our tensor notation is modified in this paper from that in [14] in that here we replace $\alpha\bar{\beta}$, $\bar{\beta}$, etc., as superscripts or subscripts by $\alpha\beta'$, β', etc. respectively.

4. A sufficient condition for vanishing cohomology. Kodaira [14] has demonstrated by means of a method due to Bochner [5], a useful sufficient condition for the vanishing of certain cohomology groups of a compact Kähler variety with coefficients in the sheaf of germs of holomorphic p-forms with coefficients in a complex line bundle. We demonstrate here analogous results useful for our purposes. For the most part, we are able simply to copy down Kodaira's formulas.

Let $\mathcal{V}$ be a complex analytic V-manifold of complex dimension n carrying the Kähler metric γ (see [2]). Since for each l. u. s. $\{U, G, v\}$, γ defines a G-invariant Kähler metric in U, it is easily seen that we may define covariant differentiation of alternating tensors on $\mathcal{V}$ by means of the usual formulas.

Let B be a complex line bundle over X and let $\mathfrak{a}$ be a C^∞ metric for B. If $\{U, G, v\}$ is a l. u. s., we define

$$X_{\alpha\beta'} = \partial_\alpha \bar{\partial}_\beta \log \mathfrak{a}_U^{-1}, \text{ in } U,$$

where $\partial_\alpha = \partial/\partial z^\alpha$ and $\bar{\partial}_\beta = \partial/\partial \bar{z}^\beta$. Let $R^\sigma{}_{\tau\alpha'\beta} = \bar{\partial}_\alpha(\sum \gamma^{\sigma\nu'}\partial_\beta \gamma_{\tau\nu'})$ (where $\gamma^{\sigma\nu'}$ is defined by $\sum \gamma^{\sigma\nu'}\gamma_{\tau\nu'} = \delta^\sigma{}_\tau$, $\gamma_{\tau\nu}{}'$ being the metric tensor and $\delta^\sigma{}_\tau$ the Kronecker symbol) and let $R_{\alpha'\beta} = \sum R^\tau{}_{\tau\alpha'\beta}$ be the Ricci tensor. Define $R_{\alpha\beta'} = \bar{R}_{\alpha'\beta}$. It is easily seen that

$$R_{\alpha\beta'} = \partial_\alpha \bar{\partial}_\beta \log[\det(\gamma_{\mu\nu'})],$$

as in Section 3. In a given system of local coordinates, we denote covariant differentiation with respect to z^α and $z^{\beta'}$ by ∇_α and $\nabla_{\beta'}$ respectively. Then if ϕ is a C^∞ form of type (r,s) on $\mathcal{V}$ with coefficients in B, we define[4]

$$\xi_{U\mu'} = \mathfrak{a}_U \sum \nabla_{\mu'} \phi_{U\tau_1\cdots\tau_r\alpha'_1\cdots\alpha'_s} \phi_U{}^{\tau_1\cdots\tau_r\alpha'_1\cdots\alpha'_s},$$

---

[4] For reasons of naturality we have always spoken of a metric for the bundle, whereas Kodaira (see [14]) speaks of a cross-section of a certain positive real line bundle. One is simply numerically the reciprocal of the other.

as in [14]. where ϕ_U represent ϕ in U and

$$\phi_U{}^{\tau_1\cdots\tau_r\alpha'_1\cdots\alpha'_s}=\sum\gamma^{\tau_1\sigma'_1}\cdot\ \cdot\ \cdot\gamma^{\tau_r\sigma'_r}\gamma^{\beta_1\alpha'_1}\cdot\ \cdot\ \cdot\gamma^{\beta_s\alpha'_s}\bar{\phi}_{U\sigma_1\cdots\sigma_r\beta'_1\cdots\beta'_s},$$

so that ξ defined in U by $\xi_U=\sum\xi_{U\mu'}dz^{\mu'}$ is a C^∞ 1-form on $\mathcal{V}$. If, moreover, ϕ is harmonic (i. e., $\square\phi=0$), we have from [14] that in U

$$\begin{aligned}-\delta\xi_U&=\sum\gamma^{\lambda\mu'}\nabla_\lambda\xi_{U\mu'}\\&=\sum s(\delta^\sigma{}_\tau[\mathrm{X}^{\beta'}{}_{\alpha'}-R^{*\beta'}{}_{\alpha'}]+rR^\sigma{}_{\tau\alpha'}{}^{\beta'})a_U\phi_{U\sigma\tau_2\cdots\tau_r\beta'\alpha'_2\cdots\alpha'_s}\bar{\phi}_U{}^{\tau\tau_2\cdots\tau_r\alpha'\alpha'_2\cdots\alpha'_s}\\&\qquad+\#=A+\#,\end{aligned}$$

where $\#$ is a non-negative quantity, and where $\mathrm{X}^{\beta'}{}_{\alpha'}=\sum\gamma^{\lambda\beta'}\mathrm{X}_{\lambda\alpha'}$ and $R^\sigma{}_{\tau\alpha'}{}^{\beta'}=\sum\gamma^{\lambda\beta'}R^\sigma{}_{\tau\alpha'\lambda}$. If we denote by 1 the function on $\mathcal{V}$ which is equal to 1 at each point, then $*1=dV$, the $2n$-form on $\mathcal{V}$ which represents the measure associated with γ (see [2]). We now suppose $\mathcal{V}$ is compact and obtain [2]

$$\int_{\mathcal{V}}\delta\xi*1=\pm\int_{\mathcal{V}}d(*\xi)=0.$$

Therefore $0=\int_{\mathcal{V}}(A+\#)*1$, or since $\#\geqq 0$, $\int_{\mathcal{V}}A*1\leqq 0$. We give a partial ordering to the Hermitian forms on $\mathcal{V}$ by writing $\mathrm{X}_1>\mathrm{X}_2$ for the Hermitian forms X_1 and X_2 if $\mathrm{X}_1-\mathrm{X}_2$ is positive definite at each point of $\mathcal{V}$. From an examination of A, we see that if the form $(\mathrm{X}_{\alpha\beta'})$ is sufficiently high in this partial ordering, then we must have $\phi\equiv 0$, for otherwise $\int_{\mathcal{V}}A*1$ would be positive. In particular, if $r=0$, it is enough to have $\mathrm{X}-R>0$. Hence, if there exists a metric a for B such that $\mathrm{X}-R>0$, we have, by Theorem D-K, that

$$H^s(\mathcal{V},\Omega^0(B))=0,\quad s\geqq 1. \tag{1}$$

Using the notation and results of Section 3 we may assert that (1) holds if $B-K$ is a positive bundle.

We observe that if $\mathcal{V}$ carries a positive complex line bundle B, then $\mathcal{V}$ is automatically Kähler. For if a is a metric for B such that the form γ, defined by $\gamma_U=id'd''\log a_U{}^{-1}$, is positive definite, then γ exhibits a Kähler metric for $\mathcal{V}$.

Let $\mathfrak{D}$ be a bounded domain in C^n and let G be a properly discontinuous group of complex analytic automorphisms of $\mathfrak{D}$ such that $\mathfrak{D}/G$ is compact. The canonical bundle for $\mathfrak{D}/G$ is positive (see Section 3), and if k is an integer, the cross-sections of kK are just the automorphic forms of weight k, while $\Omega^0(kK)$ is just the sheaf of germs of automorphic forms of weight k. If $k \geqq 2$, $kK - K = (k-1)K > 0$, and therefore

$$H^s(\mathfrak{D}/G, \Omega^0(kK)) = 0, \quad s \geqq 1.$$

This result is well known for $n = 1$ and has been proved by Kodaira for arbitrary n in case G acts without fixed points, but to the best of our knowledge has been only conjectured in the general case (see [20], exposé XX).

5. The quadratic transform [15]. Let $\mathfrak{V}$ be an n-dimensional complex analytic V-manifold and let $x_0^* \in \mathfrak{V}$. Let $\{U, G, v\}$ be a l. u. s. such that $x_0^* \in \bar{U}$ and such that $v^{-1}(x_0^*)$ consists of a single point x_0. We may assume that x_0 is the origin of C^n and that G acts as a finite linear group on C^n. We denote the complex coordinates in C^n by $z^1, \cdots, z^n$ and let $U_i = \{(z^1, \cdots, z^n) \mid (z^1, \cdots, z^n) \in U, z^i \neq 0\}$. By making an appropriate choice of coordinates (we may subject $z^1, \cdots, z^n$ to an arbitrary non-singular linear transformation if necessary) we may assume that $\bigcup_{i=1}^{n} (\bigcap_{g \in G} gU_i) = U - x_0$. This is equivalent to saying that the homogeneous polnomials $P_i(z) = \prod_{g \in G} (gz)^i$, $i = 1, \cdots, n$, $z \in C^n$. have only the trivial zero in common, where $(gz)^i$ is the i-th coordinate of gz. If x is any point of U, we let $z_x^1, \cdots, z_x^n$ denote the coordinates with center at x defined by $z_x^i(y) = z^i(y) - z^i(x)$, $y \in U$, and let G_x be the subgroup of G leaving x fixed. It is clear that the polynomials $P_x^i(z) = \prod_{g \in G_x} (gz)_x^i$, $i = 1, \cdots, n$, $z \in C^n$, where $(gz)_x^i$ is the i-th coordinate of gz in the coordinates $\{z_x^i\}$, have only the trivial zero in common. If U_x is a sufficiently small neighborhood of x in U, such that $G_x U_x = U_x$ and $gU_x \cap U_x$ is empty if $g \in G - G_x$, we may take $\{U_x, G_x, v_x\}$ as a l. u. s. for the neighborhood $\bar{U}_x = v(U_x)$ of $x^* = v(x)$, where v_x is the restriction of v to U_x. Then the following construction, which we carry out for x_0^* using the l. u. s. $\{U, G, v\}$ holds equally well for x^* using the l. u. s. $\{U_x, G_x, v_x\}$.

Let S be the $(n-1)$-dimensional complex projective space with homogeneous coordinates $(t^1, \cdots, t^n)$. Consider the product manifold $\Pi = U \times S$ and let W be the non-singular subvariety (of complex dimension n) of Π determined by

$$W = \{(z, t) \mid z^i t^j - z^j t^i = 0, i, j = 1, \cdots, n\}.$$

The analytic map $\pi\colon W \to U$ of W onto U given by $\pi(z, t) = z$ has the easily seen properties that it is a biregular mapping of $W - \pi^{-1}(x_0)$ onto $U - x_0$ and that $\pi^{-1}(x_0)$ is a non-singular subvariety of W which is naturally biregularly equivalent to S. Therefore without material risk of confusion we denote $\pi^{-1}(x_0)$ by S. We also use S to denote the prime divisor on W determined by S.

We observe some elementary facts about W and the subvariety or divisor S of W. Let $l_i = \{(z,t) \mid (z,t) \in W, t^i = 0\}$ and let $W_i = W - l_i$. Then on W_i we may choose

$$\text{(I)} \qquad (t^1/t^i), \cdots, (t^{i-1}/t^i), z^i, (t^{i+1}/t^i), \cdots, (t^n/t^i)$$

as local coordinates;

$$\text{(II)} \qquad z^j = z^i(t^j/t^i), j \neq i, \text{ in } W_i,$$

so that

$$\text{(III)} \quad dz^1 \wedge \cdots \wedge dz^n = (z^i)^{n-1} d(t^1/t^i) \wedge \cdots \wedge dz^i \wedge \cdots \wedge d(t^n/t^i) \text{ in } W_i.$$

Let $w \in W$ and let S_w be the ideal in the ring of local holomorphic functions $\mathfrak{O}_w$ at w consisting of functions which are locally multiples of S, and for any function f holomorphic at w, let f_w denote the principal ideal (f) in $\mathfrak{O}_w$. At each point of W_i, $S_w = (z^i)_w$. Obviously $z^1, \cdots, z^n$ are holomorphic functions on W. Let P be a homogeneous polynomial in $z^1, \cdots, z_n$ of degree q. In view of (II) we may write

$$P = (z^i)^q P^*(t^j/t^i) \text{ in } W_i,$$

where P^* is a polynomial in the (t^j/t^i)'s, $j \neq i$. From this it is easy to see that if P is a non-zero, homogeneous polynomial of degree q in $z^1, \cdots, z^n$, then at any point $w \in S_i$, P is divisible by z^i to precisely the q-th power.

We now show that the group G acting on U can be lifted in a unique way to a finite group of complex analytic transformations of W; i. e., to each $g \in G$ we may assign a unique transformation g' of W such that $\pi g' = g\pi$. It will follow trivially that $g \to g'$ is an isomorphism of G onto a group G' of complex analytic transformations of W. First of all, $g \in G$ acts on the local coordinates of U as a linear transformation:

$$(gz)^i = \sum g^i{}_\alpha z^\alpha.$$

For $(z,t) \in \Pi$ we define $g'(z,t) = (gz, gt)$, where $(gt)^i = \sum g^i{}_\alpha t^\alpha$. Then $(z,t) \in W$ if and only if $g'(z,t) \in W$ since

$$(gt)^j (gz)^i - (gt)^i (gz)^j = \sum_{\alpha,\beta} g^i{}_\alpha g^j{}_\beta (t^\beta z^\alpha - t^\alpha z^\beta).$$

Thus g' gives a biregular map of W onto itself which we also denote by g'. It is obvious that $(g_1 g_2)' = g_1' g_2'$ and that the mapping $g \to g'$ is an isomorphism, and it is easily seen that the complex analytic transformation g' of W satisfying $\pi g' = g\pi$ is unique.

It is clear that W/G' is a V-manifold. We let p be the canonical projection of W onto W/G' and define $\theta\colon (W - S)/G' \to \mathcal{V} - x_0{}^*$ by $\theta = \phi \circ \pi \circ p^{-1}$. Then we denote by $\mathfrak{Q}_{x_0{}^*}(\mathcal{V})$ the complex analytic V-manifold obtained from $W/G' \cup \mathcal{V} - x_0{}^*$ by identifying $\tilde{w} \in (W - S)/G'$ with $\theta(\tilde{w})$. When there is no danger of confusion, we denote $\mathfrak{Q}_{x_0{}^*}(\mathcal{V})$ by $\mathcal{V}_{x_0}$. We let $\mathcal{P}$ denote the natural projection of $\mathcal{V}_{x_0}$ onto $\mathcal{V}$ (defined by $\mathcal{P}(S) = x_0{}^*$ and $\mathcal{P}(x) = x$ if $x \in \mathcal{V} - x_0{}^*$). It is clear that if B is a V-bundle on $\mathcal{V}$, then B and $\mathcal{P}$ together define a V-bundle $\mathcal{P}^{-1}(B) = B_{[x_0]}$ having the same fibre, group, and differentiable structure as B. We denote the canonical bundle on $\mathcal{V}_{x_0}$ by K_{x_0} and denote by S^* the divisor on $\mathcal{V}_{x_0}$ which is induced by the divisor S on W (this definition is legitimate since S is stable under G'). It follows from (III) that

$$K_{x_0} = (n-1)\{S^*\} + K_{[x_0]} \tag{IV}$$

As remarked in Section 3, $m_0\{S^*\}$ is an absolute bundle. It turns out that $m\{S^*\}$ is an absolute bundle, where $m = \operatorname{ord} G$. We now construct coordinate transformations for $m\{S^*\}$. Let $\mathcal{W}_i = \bigcap_{g \in G} g'W_i$, $i = 1, \cdots, n$. Since the polynomials $\boldsymbol{P}_i$, $i = 1, \cdots n$, have only the trivial zero in common, it follows that $\mathcal{W}_1, \cdots, \mathcal{W}_n$ cover W. If $a_1, \cdots, a_n$ are complex numbers, then at each $w = (z, t) \in W$ such that $\sum a_j t^j \neq 0$ we have $(\sum a_j z^j)_w = S_w$. We put $f^i(z, t) = f^i(z) = \prod_{g \in G} (gz)^i$, $i = 1, \cdots, n$. If $w = (z, t) \in \mathcal{W}_i$, then $(mS)_w = f^i{}_w$. Moreover, each f^i is G-invariant. The open sets $U_0 = \mathcal{V} - x_0$ and $U_i = \mathcal{W}_i/G'$, $i = 1, \cdots, n$, viewed as components of the identification space $\mathcal{V}_{x_0}$, cover $\mathcal{V}_{x_0}$. We define $f^0 = 1$ on all of $\mathcal{V} - x_0$. By our remarks in Section 3, the absolute bundle $\{mS^*\}$ may be viewed as the complex line bundle over $\mathcal{V}_{x_0}$ defined by the system of coordinate neighborhoods $\{U_i\}$ and coordinate transformations (or transition functions) $\{f_{ij}\}$, where f_{ij} is the non-zero holomorphic function in $U_i \cap U_j$ defined by $f_{ij} = f^i/f^j$.

If x is any point of U, we carry out the same construction for x using the l. u. s. $\{U_x, G_x, v_x\}$ and denote the entities corresponding to U_i, W, W_i, G', $\mathcal{W}_i$, l_i, K_{x_0}, $K_{[x_0]}$, f^i, f_{ij}, m, π, $\mathcal{P}$, $\mathcal{V}_{x_0}$, and S in the above construction by U_{xi}, W_x, W_{xi}, $G_x{}'$, $\mathcal{W}_{xi}$, $l^x{}_i$, K_x, $K_{[x]}$, $f_x{}^i$, f_{xij}, m_x, π_x, $\mathcal{P}_x$, $\mathcal{V}_x$, and S_x respectively. Let U^* be a neighborhood of x_0 in U such that $GU^* = U^*$. Let $\mathsf{M} = \{(x, y) \mid (x, y) \in U^* \times U, y \in Gx\}$. Then by a singular G-form of class C^∞ and type (p, q) on U with respect to U^*, we mean a C^∞ form ψ on $U^* \times U - \mathsf{M}$ such that for fixed $x \in U^*$, ψ_x defined on $U - G_x$ by $\psi_x(y)$

$=\psi(x,y)$ is a G-invariant, C^∞ form of type (p,q). Using this notation we have the

Theorem of Continuity. *There exists a neighborhood U^* of x_0 stable under G with compact closure in U, and a real, singular G-form ψ of class C^∞ and of type $(1,1)$ on U with respect to U^* such that:*

(1) *For each $x \in U^*$, ψ_x induces in a natural manner a real C^∞ form of type $(1,1)$ on $\mathfrak{P}_x^{-1}(v(U)-v(x))$ which may be extended to a C^∞ form ψ_x' on $\mathfrak{P}_x^{-1}(\mathfrak{V}-v(x))$ by defining $\psi_x'=0$ outside $\mathfrak{P}_x^{-1}(v(U)-v(x))$;*

(2) *ψ_x' has a unique extension to a C^∞ form ψ_x' on all of $\mathfrak{V}_x$, and ψ_x' belongs to the characteristic class of $\{-m_xS_x^*\}$.*

Proof. We know that there exist positive real numbers $M \geqq 1$ and $\mu \leqq 1$ such that given any $x,y \in U$ and any $g \in G$ we have $\mu\,|x-y| \leqq |gx-gy| \leqq M\,|x-y|$, where $|x-y|$ is the Euclidean distance between x and y in the given coordinates on U.

Let $\epsilon > 0$ be such that U contains a closed Euclidean ball of radius 10ϵ. Let ρ be a C^∞ function on the non-negative real axis such that

$$\rho(r^2) = \begin{cases} r^2 \text{ for } r < 6\epsilon\mu, \\ \text{a non-decreasing function in } r \text{ for } 6\epsilon\mu \leqq r \leqq 7\epsilon\mu, \\ \text{a constant } C \text{ for } r > 7\epsilon\mu. \end{cases}$$

Let U^* be a neighborhood of x_0 stable under G such that U^* is contained in the Euclidean ball of radius $\epsilon\mu/M$ about x_0.

Define Λ on $U^* \times U$ by $\Lambda(x,y) = \Pi_{g\in G}\,\rho(|x-gy|^2)$. We note that we may write $\Lambda(x,y) = \Pi_\kappa[\Pi_{g\in G_x}(|x-g\kappa y|^2)]$, where κ runs over a system of representatives of the right cosets of G_x in G. For fixed $x \in U^*$ we put $\psi_x(y) = \psi(x,y) = \frac{i}{2\pi}d'd''\log\Lambda(x,y)$, $y \in U - Gx$. It is evident that $\psi_x(y)$ is a C^∞ real form of type $(1,1)$ in $U - Gx$ invariant under G, and that $\psi_x(y)$ vanishes if $|y-x_0| = |y| > 8\epsilon$. This being the case, assertion (1) is obvious.

Let $x \in U^*$ and let N be a neighborhood of x stable under G_x such that $gN \cap N$ is empty if $g \in G - G_x$ and such that $N \subset U^*$. For any real number $r > 0$, let $\beta(x,r)$ denote the open Euclidean ball of radius r about x. We choose neighborhoods N_1, N_2, N_3 of x stable under G_x and positive numbers $\delta > \delta_1 > \delta_2 > 0$ such that $\operatorname{clos}(N_3) \subset \beta(x,\delta_2)$, $\operatorname{clos}(\beta(x,\delta_2)) \subset N_2$, $\operatorname{clos}(N_2) \subset \beta(x,\delta_1)$, $\operatorname{clos}(\beta(x,\delta_1)) \subset N_1$, $\operatorname{clos}(N_1) \subset \beta(x,\delta)$, $\operatorname{clos}(\beta(x,\delta)) \subset N$. Let ρ_x be a C^∞ function on the non-negative real axis such that

$$\rho_x(r^2) = \begin{cases} r^2 \text{ for } r < \delta_2, \\ \text{a non-decreasing function in } r \text{ for } \delta_2 < r < \delta_1, \\ \text{a constant } C_x \text{ if } r > \delta_1. \end{cases}$$

We define

$$\Xi_x(y) = \frac{i}{2\pi} d'd'' \log[\prod_{g \in G_x} \rho_x(|x - gy|^2)], \quad y \in N - x,$$

and define $\Xi_x(y) = 0$ if $y \in U - N$. Let $\Psi_x(y) = \sum'_{\kappa} \kappa^* \Xi_x(\kappa y)$ in $U - Gx$, where κ again runs over a system of right coset representatives of G_x in G. Then

$$\Psi_x(y) = \frac{i}{2\pi} d'd'' \log \prod_{g \in G} \rho_x(|x - gy|^2), \quad y \in U - Gx,$$

and $(\psi_x - \Psi_x)(y) = \frac{i}{2\pi} d'd'' \log E_x(y)$, where

$$E_x(y) = \prod_{g \in G} [\rho(|x - gy|^2)/\rho_x(|x - gy|^2)]$$

is a non-vanishing, G-invariant, C^∞ function in U having the constant value $(C/C_x)^m$ for $|y - x_0| > 8\epsilon$, where $m = \operatorname{ord} G$. Therefore ψ_x and Ψ_x induce forms on $\mathfrak{P}_x^{-1}(v(U) - v(x))$ which differ by a form X which can be extended to a C^∞ exact form (i.e., $X = d\theta$) on all of $\mathfrak{V}_x$. Hence it is sufficient to show that the form Ψ_x' on $\mathfrak{V}_x - \mathfrak{P}_x^{-1}(v(x))$, induced on $\mathfrak{P}_x^{-1}(v(U) - v(x))$ by Ψ_x and defined to be 0 outside of $\mathfrak{P}_x^{-1}(v(U))$, has an extension to a form on $\mathfrak{V}_x$ belonging to the characteristic class of $\{-m_x S_x^*\}$, for if the extension exists, it is obviously unique by continuity.

We define T_x on $\mathfrak{V}$ by $T_x(v(y)) = \prod_{g \in G} \rho_x(|x - gy|^2)$ if $y \in U$ and $T_x(\eta) = C_x^m$ if $\eta \notin v(U)$. Then T_x is clearly a well-defined function of class C^∞ on $\mathfrak{V}$ which is non-vanishing on $\mathfrak{V} - v(x)$. Moreover, in N_3,

$$T_x(v(y)) = (\prod_{g \in G_x} |x - gy|^2) C_x^{(m - m_x)}.$$

It is obvious that $\Psi_x' = \frac{i}{2\pi} d'd'' \log(T_x \circ \mathfrak{P}_x)$ on $\mathfrak{P}_x^{-1}(\mathfrak{V} - v(x))$, $\circ$ denoting the composition of functions. $\mathfrak{Q}_x(\mathfrak{V}) = \mathfrak{V}_x$ is supposed to have been constructed with the complex coordinates $z_x^1, \cdots, z_x^n$ in N_3. Hence W_x is the non-singular subvariety of $N_3 \times S$ defined by $z_x^j t^i - z_x^i t^j = 0$, $i, j = 1, \cdots, n$; and $S_x = \pi_x^{-1}(x)$ is the non-singular prime divisor on W_x such that $(S_x)_w = (\sum a_j z_x^j)_w$ for each $w = (z, t) \in W_x$ such that $\sum a_j t^j \neq 0$. For brevity let $(z_x^1, \cdots, z_x^n) = z_x$. We also write $(gz_x)^i(y) = z_x^i(gy)$ for $g \in G_x$, so that $(gz_x)^i = \sum g^i{}_j z_x^j$ since G_x acts linearly in the coordinates $\{z_x^i\}$. We now construct a C^∞ metric $\{a_i\}$ for the bundle $\{-m_x S_x^*\}$, where a_i will be a C^∞ function in the i-th coordinate neighborhood U_{xi} of $\{-m_x S_x^*\}$. We define

$$a_i(\tilde{w})^{-1} = [\prod_{g \in G_x} (\sum_{\nu=1}^{n} |(gt)^\nu/(gt)^i|^2)] C_x^{(m - m_x)},$$

$i = 1, \cdots, n$, if $\tilde{w}$ is the natural image in $U_{xi} = \mathcal{W}_{xi}/G_x'$ of $w = (z_x, t) \in \mathcal{W}_{xi}$, and define $\mathfrak{a}_0(\eta)^{-1} = T_x(\eta)$ if $\eta \in U_{x_0} = \mathcal{V}_x - S_x$. Using the fact that $z_x{}^j t^i - z_x{}^i t^j = 0$ on W_x, $i, j = 1, \cdots, n$, we obtain easily that $\mathfrak{a}_i/\mathfrak{a}_j = |f_{xij}|^{-2}$ on $U_{xi} \cap U_{xj}$, $i, j = 0, 1, \cdots, n$. Consequently, the form ϕ on $\mathcal{V}_x$ defined on U_{xi} by $\phi = \frac{i}{2\pi} d'd'' \log \mathfrak{a}_i^{-1}$ is a C^∞ real form of type $(1, 1)$ in the characteristic class of $\{-m_x S_x{}^*\}$, and since $\phi = \Psi_x'$ on $\mathcal{V}_x - S_x$, our theorem is proved.

We use the notations of the statement and proof of the continuity theorem in the following discussion.

Define ω to be the form on the $(n-1)$-dimensional projective space S which is given on the affine space $t^\nu \neq 0$ by

$$\omega = \frac{i}{2\pi} d'd'' \log(1 + \textstyle\sum_{j \neq \nu} |t^j/t^\nu|^2).$$

ω is well known to be positive definite. If $C^n - 0$ is the space of n complex variables minus the origin, ω induces the form $\omega' = \frac{i}{2\pi} d'd'' \log(\sum |z^i|^2)$ on $C^n - 0$ under the natural projection of $C^n - 0$ onto S, and ω' is positive semi-definite. It follows from the construction of ρ and $\psi_x(y)$ that ψ_x is a positive semi-definite form in the regions $|y - x_0| < 5\epsilon\mu/M$, $|y - x_0| > 9\epsilon$ for each $x \in \bar{U}^*$. In the compact subspace

$$\{(x, y) \mid x \in \bar{U}^*, 5\epsilon\mu/M \leqq |y - x_0| \leqq 9\epsilon\}$$

of $\bar{U}^* \times U$, $\psi_x(y)$ depends continuously on x and y. Therefore, if α is a positive definite form in the region $5\epsilon\mu/M \leqq |y - x_0| \leqq 9\epsilon$, there exists a real number $R > 0$ such that if $r \geqq R$ and $x \in \bar{U}^*$, then $r\alpha + \psi_x$ is positive definite in this region. Consequently, if α is a positive definite C^∞ form on $\mathcal{V}$, there exists an $R > 0$ such that $r\alpha + \psi_x > 0$ in $\mathcal{V} - v(x)$, for $r \geqq R$, where we use ψ_x to denote the form previously defined on $U - Gx$ as well as the form which the latter induces on $\mathcal{V} - v(x)$ when we define $\psi_x = 0$ outside $v(U)$. On $\mathcal{W}_{xi}$ we have

$$\psi_x' = \frac{i}{2\pi} d'd'' \log[\textstyle\prod_{g \in G_x} (\sum_{\nu=1}^{n} |(gt)^\nu/(gt)^i|^2)],$$

and the latter expression, which we denote by $\omega_i(t)$, is clearly positive definite on the subset $S_{xi} = \{t \mid t \in S, \prod_{g \in G_x} (gt)^i \neq 0\}$ of S. On the other hand, $r\alpha > 0$ on N_3. Hence $\omega_i(t) + r\alpha > 0$ on $N_3 \times S_{xi}$, and if we let ι_i be the inclusion map of $\mathcal{W}_{xi}$ into $N_3 \times S_{xi}$, we have $\mathcal{P}_x{}^*(r\alpha) + \psi_x' = \iota_i{}^*(\omega_i + r\alpha) > 0$ Moreover, $\mathcal{P}_x$ is an isomorphism of V-manifolds outside $S_x/G_x = \mathcal{P}_x{}^{-1}(v(x))$, so that $\mathcal{P}_x{}^* r\alpha + \psi_x' > 0$ on $\mathcal{V}_x - S_x$, and therefore $\mathcal{P}_x{}^* r\alpha + \psi_x' > 0$ on all $\mathcal{V}_x$.

If F is a complex line bundle over $\mathcal{V}$ and $\mathfrak{a}$ a C^∞ metric for F, then under the map $\mathfrak{P}_x$, F and α induce, respectively, a complex line bundle F' on $\mathfrak{V}_x$ and a metric α' for F'. It is trivial that $d'd''\log\alpha' = \mathfrak{P}_x{}^* d'd''\log\alpha$, where $\mathfrak{P}_x{}^*$ is the mapping of differential forms dual to $\mathfrak{P}_x$. Suppose now that there exists a positive complex line bundle F on $\mathfrak{V}$. Then there exists a C^∞ metric α for F such that $\Upsilon = \frac{i}{2\pi} d'd''\log\alpha^{-1}$ is positive definite on $\mathfrak{V}$. There exists a positive integer $l(x_0)$ such that $l(x_0)\Upsilon + \psi_x > 0$ in the region $5\epsilon\mu/M \leqq |y - x_0| \leqq 9\epsilon$, for all $x \in U^* = U^*(x_0)$, so that $\mathfrak{P}_x{}^*(l(x_0)\Upsilon) + \psi_x' > 0$ on $\mathfrak{V}_x$. We observe that $\mathfrak{P}_x{}^*(l(x_0)\Upsilon) + \psi_x'$ is in the characteristic class of $l(x_0)F_{[x]} - \{m_x S_x{}^*\}$.

We now assume that $\mathfrak{V}$ is compact and let k be any integer > 0. Let $F_1 = l(x_0)F$ and put $F^* = (n + q(x_0))F_1$, where $q(x_0)$ is an integer at our disposal. Then by (IV),

$$\begin{aligned} m_0(F^*{}_{[x]} - k\{m_x S_x{}^*\}) - m_0 K_x = {} & [km_0 + (n-1)p_x](F_{1[x]} - \{m_x S_x{}^*\}) \\ & + [m_0(n + q(x_0)) - km_0 - (n-1)p_x]F_{1[x]} - m_0 K_{[x]}, \end{aligned}$$

where $p_x m_x = m = \operatorname{ord} G$. p_x is a divisor of m, so the number of distinct p_x's for $x \in U$ is finite. Choose $q(x_0)$ such that

$$[m_0(n + q(x_0)) - km_0 - (n-1)p_x]F_1 - m_0 K > 0$$

for all $x \in U$. Then $m_0(F^*{}_{[x]} - k\{m_x S_x{}^*\}) - m_0 K_x > 0$, since $F_{1[x]} - \{m_x S_x{}^*\} > 0$, and therefore $(F^*{}_{[x]} - k\{m_x S_x{}^*\}) - K_x > 0$ for all $x \in U^*$; for if α is a metric for $m_0(F^*{}_{[x]} - k\{m_x S_x{}^*\}) - m_0 K_x$, α^{1/m_0} is a metric for $(F^*{}_{[x]} - k\{m_x S_x{}^*\}) - K_x$. Thus we obtain

AUXILIARY THEOREM I. *Let $\mathfrak{V}$ be a compact, complex analytic V-manifold. Assume there exists a positive line bundle on $\mathfrak{V}$. Choose a finite number of points $x_0{}^1, \cdots, x_0{}^p$ with neighborhoods $U^*(x_0{}^i)$ (as above) such that $\mathfrak{V}$ is covered by the natural images of $U^*(x_0{}^i)$, $i = 1, \cdots, p$, and for each i let an integer $k_i \geqq 0$ be given. Then there exists a positive complex line bundle F on $\mathfrak{V}$ such that*

$$(F_{[x]} - k_i\{m_x S_x{}^*\}) - K_x > 0$$

for $x \in U^*(x_0{}^i)$, $i = 1, \cdots, p$.

Let $x^*, y^* \in \mathfrak{V}$, $x^* \neq y^*$. We construct $\mathfrak{Q}_{x^*}(\mathfrak{V})$, denote $\mathfrak{P}_x{}^{-1}(y^*)$ again by y^* and construct $\mathfrak{Q}_{y^*}(\mathfrak{Q}_{x^*}(\mathfrak{V}))$. We let $S_x{}^*$ and $S_y{}^*$ denote, respectively, the divisors on $\mathfrak{Q}_{y^*}(\mathfrak{Q}_{x^*}(\mathfrak{V}))$ associated (as before) with the $(n-1)$-dimensional complex projective spaces by which x and y are replaced in local uniformizing systems $\{U_1, G_1, \nu_1\}$ and $\{U_2, G_2, \nu_2\}$ such that $\nu_1(x) = x^*$ and

$v_2(y) = y^*$. These definitions are legitimated by the fact that if $\mathfrak{V}$ is a V-manifold, and $\mathfrak{V}_x$, S_x, and $\mathfrak{P}_x$ have their previous meanings, then $\mathfrak{P}_x$ is an isomorphism of $\mathfrak{V}_x - S_x/G_x'$ onto $\mathfrak{V} - x^*$. We denote by K_{xy} the canonical bundle on $\mathfrak{Q}_{y^*}(\mathfrak{Q}_{x^*}(\mathfrak{V}))$. Then computations entirely similar to those above yield (see Kodaira [15], p. 33, Lemma 2):

AUXILIARY THEOREM II. *Let $\mathfrak{V}$ be a compact, complex analytic V-manifold and assume there exists a positive complex line bundle F on $\mathfrak{V}$. Then for all sufficiently high multiples mF and all $x^*, y^* \in \mathfrak{V}$, such that $x^* \neq y^*$, we have*

$$(mF_{[xy]} - \{m_x S_x^*\} - \{m_y S_y^*\}) - K_{xy} > 0,$$

where $F_{[xy]}$ is the bundle induced on $\mathfrak{Q}_{y^*}(\mathfrak{Q}_{x^*}(\mathfrak{V}))$ by F under the mapping $\mathfrak{P}_x \mathfrak{P}_y$, and m_x and m_y have their usual meanings.

6. Holomorphic cross-sections of a positive complex line bundle having prescribed properties. The results of this section are established for absolute complex line bundles, the question of their validity for general complex line bundles having no immediate importance for our purposes. Let $\mathfrak{V}$ be a compact V-manifold. We shall suppose that there exists a positive complex line bundle over $\mathfrak{V}$, from which it follows immediately that there exists a positive absolute complex line bundle over $\mathfrak{V}$. In what follows we will always assume that a given absolute complex line bundle is defined by a system of neighborhoods $\{\bar{U}_i\}$, where $\{U_i, G_i, v_i\}$ is a l. u. s., and a system of holomorphic coordinate functions $\{f_{ij}\}$; then for each $g \in G_i$, the map $h_{U_i}(g)$ of $U_i \times C$ onto itself is given by $h_{U_i}(g)(z, c) = (g^{-1}z, c)$ (see [2]). Thus a holomorphic cross-section of the complex line bundle is given by prescribing, for each i, a G_i-invariant holomorphic function f_i in U_i such that on $\bar{U}_i \cap \bar{U}_j$, $f_i = f_{ij} f_j$. If we are given any finite number of absolute complex line bundles, we may assume they have a common system of such coordinate neighborhoods.

BASIC EXISTENCE THEOREM. *Using the above notation and the notation of Section 5, let $x \in U_l$ and let k be a positive integer. Suppose that F is a positive complex line bundle on $\mathfrak{V}$ such that $(F_{[x]} - k\{m_x S_x\}) - K_x > 0$. Let $P(z_x^1, \cdots, z_x^n)$ be a polynomial invariant under G_x of total degree $< km_x$ in the coordinates $\{z_x^i\}$ with center at x. Then there exists a holomorphic cross-section $f = \{f_i\}$ of F such that $P - f_l$ has a zero of order $\geqq km_x$ at x.*

Proof. First of all, it is easily seen that it suffices to prove our theorem for a bundle complex analytically V-equivalent to F. In what follows, we denote all members of a family of complex analytically V-equivalent bundles by the same letter. Let $\{V_e'\}$ be a common system of coordinate neighborhoods for the three absolute complex line bundles $\{m_xS_x^*\}$, $F_{[x]}$ and $F_{[x]}-\{m_xS_x^*\}$ on $\mathcal{V}_x$. Let $U_i'=\mathfrak{P}_x^{-1}(\tilde{U}_i)$. Then $S_x/G_x'\subset U_i'$ and it is clear that $F_{[x]}$ is a product bundle over U_i'. Hence a holomorphic section σ of $F_{[x]}$ over any open subset $\mathcal{O}$ of U_i' may be viewed as a single holomorphic function σ_i on $\mathcal{O}$.

If Ω is any sheaf over $\mathcal{V}$ or $\mathcal{V}_x$, then in what follows we denote the stalk of Ω over the point y^* by Ω_{y^*}. We have defined the two sheaves $\Omega^0(F_{[x]})$ and $\Omega^0(F_{[x]}-k\{m_xS_x^*\})$ which are the sheaves of germs of holomorphic cross-sections of the two bundles. We now define an isomorphism of $\Omega^0(F_{[x]}-\{m_xS_x^*\})$ onto $\Omega^0(F_{[x]})$. This isomorphism arises by multiplication by a suitable cross-section of the bundle $k\{m_xS_x^*\}$. Let $y^*\in\mathcal{V}_x$ and let $\alpha_{y^*}\in\Omega^0(F_{[x]}-\{m_xS_x^*\})_{y^*}$. Let $\{U',G',v'\}$ be a l.u.s. on $\mathcal{V}_x$ such that $y^*=v'(y)$. Then in a sufficiently small neighborhood V of y stable under G'_y, such that $gV\cap V$ is empty if $g\in G'-G'_y$, a representative of α_{y^*} is a collection of holomorphic functions α^e, α^e being defined in $v'^{-1}(V'_e)\cap V$ and invariant under G'_y, such that $\alpha^e=(b_{ef}\circ v')\alpha^f$ in $V\cap v'^{-1}(V_e')\cap v'^{-1}(V_f')$, where b_{ef} is the non-vanishing holomorphic coordinate function for $F_{[x]}-\{m_xS_x^*\}$ in $V_e'\cap V_f'$. Let s^e be the chosen invariant holomorphic function in V such that $(s^e)_w=(km_xS_x^*)_w$ at each $w\in v'^{-1}(V_e')$. Define $\beta^e=s^e\alpha^e$. Then since $\beta^e=(s^e/s^f)(b_{ef}\circ v')\beta^f$ in $v'^{-1}(V_e')\cap v'^{-1}(V_f')\cap V$, $\{\beta^e\}$ represents a germ $\beta_{y^*}\in\Omega^0(F_{[x]})_{y^*}$. We define $\mathfrak{I}:\Omega^0(F_{[x]}-k\{m_xS_x^*\})\to\Omega^0(F_{[x]})$ by $\mathfrak{I}(\alpha_{y^*})=\beta_{y^*}$, as given above. It is clear that $\mathfrak{I}$ is an isomorphism of the sheaf $\Omega^0(F_{[x]}-k\{m_xS_x^*\})$ into the sheaf $\Omega^0(F_{[x]})$. Thus we have the exact sequence of sheaves

$$\begin{aligned}0\to\Omega^0(F_{[x]}-k\{m_xS_x^*\})&\xrightarrow{\mathfrak{I}}\Omega^0(F_{[x]})\\&\xrightarrow{j}\Omega^0(F_{[x]})/\mathfrak{I}[\Omega^0(F_{[x]}-k\{m_xS_x^*\})]\to 0\end{aligned}$$

and from this we obtain the exact cohomology sequence

$$\begin{aligned}0\to\Gamma(F_{[x]}-k\{m_xS_x^*\})&\xrightarrow{\mathfrak{I}^*}\Gamma(F_{[x]})\\&\xrightarrow{j^*}\Gamma(\Omega^0(F_{[x]})/\mathfrak{I}[\Omega^0(F_{[x]}-k\{m_xS_x^*\})])\\&\xrightarrow{\delta^*}H^1(\mathcal{V}_x,\Omega^0(F_{[x]}-k\{m_xS_x^*\}))\to\cdots\end{aligned}$$

where Γ in each case stands for "(holomorphic) sections of." However, by hypothesis, $(F_{[x]}-k\{m_xS_x^*\})-K_x>0$. Hence $H^1(\mathcal{V}_x, \Omega^0(F_{[x]}-k\{m_xS_x^*\}))=0$. Therefore j^* is "onto."

We now examine the image of $\mathfrak{d}$ in $\Omega^0(F_{[x]})$. First of all, it is evident that if $\beta_{y^*}\in \operatorname{Im}(\mathfrak{d})_{y^*}$, $\beta_{y^*}=\{\beta^e\}$, then each β^e is divisible by s^e at y and so belongs to the ideal $(km_xS_x)_y$ at y. On the other hand. suppose $\beta_{y^*}=\{\beta^e\}$, where each β^e is divisible by s^e in some small neighborhood V of y stable under G'_y; we define $\alpha^e=\beta^e/s^e$ in $V\cap v'^{-1}(V_e')$. It is clear that the system $\{\alpha^e\}$ defines an $\alpha_{y^*}\in\Omega^0(F_{[x]}-k\{m_xS_x^*\})_{y^*}$ and that $\beta_{y^*}=\mathfrak{d}(\alpha_{y^*})$. Hence $\mathfrak{d}[\Omega^0(F_{[x]}-k\{m_xS_x^*\})]$ is the subsheaf of $\Omega^0(F_{[x]})$ consists of those germs β such that a representative of β is divisible by s^e at $p(\beta)$, where p is the projection of $\Omega^0(F_{[x]})$ onto $\mathcal{V}_x$.

We wish to study the module

$$\Gamma(\Omega^0(F_{[x]})/\mathfrak{d}[\Omega^0(F_{[x]}-k\{m_xS_x^*\})]).$$

In the first place, in a coordinate neighborhood V_e' of the bundle $\{m_xS_x^*\}$, the holomorphic function s^e is a unit at $y^*\in V_e'$ if $y^*\notin \mathcal{P}_x^{-1}(x^*)$. Therefore $[\Omega^0(F_{[x]})/\mathfrak{d}[\Omega^0(F_{[x]}-k\{m_xS_x^*\}]]_{y^*}=0$ if $y^*\notin\mathcal{P}_x^{-1}(x^*)$.

We return to our notation of Section 5, where $\{U_x, G_x, v_x\}$, π_x, W_x, etc. were defined, and exhibit a natural decomposition of the local ring of holomorphic functions on W_x at each point of S_x. Let

$$(z_x,t)_0=(0,\cdots,0,t_0^1,\cdots,t_0^n)\in\mathcal{W}_{xi}\cap S_x.$$

Let $t_0^j/t_0^i=a_0^j$. Then z_x^i and $[(t^j/t^i)-a_0^j]$, $j\neq i$, may be taken as local coordinates with center $(z_x,t)_0$. Let f be holomorphic on W_x at $(z_x,t)_0$. Then f is a power series in these coordinates:

$$f(z_x,t)=\textstyle\sum_{m_i;m_j,j\neq i}a_{m_i;m_1\cdots m_i'\cdots m_n}(z_x^i)^{m_i}\prod_{j\neq i}[(t^j/t^i)-a^j{}_0]^{m_j}$$

(where m_i' means "omit m_i")

$$=\textstyle\sum_{m_i<km_x;m_j,j\neq i}a_{m_i;m_1\cdots m_i'\cdots m_n}(z_x^i)^{m_i}\prod_{j\neq i}[(t^j/t^i)-a^j{}_0]^{m_j}$$

$$+\textstyle\sum_{m_i\geqq km_x;m_j,j\neq i}m_{i;m_1\cdots m_i'\cdots m_n}(z_x^i)^{m_i}\prod_{j\neq i}[(t^j/t^i)-a^j{}_0]^{m_j}$$

$$=\mathsf{A}(f)+\mathsf{B}(f).$$

This decomposition is, of course, unique in the given local coordinates at $(z_x,t)_0$ (by the uniqueness of the power series expansion of an analytic function). Moreover, suppose N is a small neighborhood of $(z_x,t)_0$ in which this series converges, $N\subset\mathcal{W}_{xi}$, and let $(z_x,t)_1=(0,\cdots,0,t_1^1,\cdots,t_1^n)\in N\cap S_x$. Then the coefficient of $(z_x^i)^{m_i}$ in the power series development of f at $(z_x,t)_1$ is a power series in the coordinates $[(t^j/t^i)-(t_1^j/t_1^i)]$, and so the decomposition of f into the sum of two analytic functions is the same as that above, in a neighborhood of $(z_x, t)_1$; this expresses, so to speak, the fact that the decomposition is "analytically continuous" on S_x. $(gt)^i \neq 0$ if $(z_x, t) \in \mathcal{W}_{xi}$ for all $g \in G_x$, and $((gz)_x{}^i)_w = (S_x)_w$ at each $w \in \mathcal{W}_{xi}$. It is thus easily seen that the decomposition is independent of the choice of i such that $(z_x, t)_0 \in \mathcal{W}_{xi}$, and that the decomposition is invariant under G_x'. It is evident that $\mathsf{B}(f)_{w_0} \subset (km_xS_x)_{w_0}$ at $w_0 \in S_x$, while $\mathsf{A}(f)_{w_0} \subset (km_xS_x)_{w_0}$ only if $\mathsf{A}(f) = 0$. As we have pointed out, $F_{[x]} \mid U_i'$ is complex analytically the product bundle, so that, if $w_0{}^* \in U_i'$, we may regard $\Omega^0(F_{[x]})_{w_0{}^*}$ as being the ring $\mathfrak{O}_{w_0{}^*}$ of local holomorphic functions at $w_0{}^*$, and if $w_0{}^*$ is the natural image in $\mathcal{V}_x$ of $w_0 \in W_x$, $\mathfrak{O}_{w_0{}^*}$ is to be identified with the ring of local holomorphic functions at w_0 invariant under G'_{w_0}, the subgroup of G_x' leaving w_0 fixed. For any function f holomorphic in a neighborhood of y^*, denote by $f_{[y^*]}$ the germ of holomorphic functions induced by f at y^*. Then since the decomposition $f \to \mathsf{A}(f) + \mathsf{B}(f)$ is invariant under the elements of G'_{w_0}, the mapping $f \to \mathsf{A}(f)$ induces a natural homomorphism $\mathsf{A}_{w_0{}^*}$ of $\Omega^0(F_{[x]})_{w_0{}^*}$ onto a submodule $\mathcal{A}_{w_0{}^*}$ of the complex module of local holomorphic functions at $w_0{}^*$ for $w_0 \in S_x$; and we then have the isomorphism

$$i_{w_0{}^*}\colon\ [\Omega^0(F_{[x]}) / \mathfrak{d}\,[\Omega^0(F_{[x]} - k\{m_xS_x{}^*\})]]_{w_0{}^*} \cong \mathcal{A}_{w_0{}^*}$$

defined by choosing a representative f of a coset α of

$$\mathfrak{d}\,[\Omega^0(F_{[x]} - k\{m_xS_x{}^*\})]_{w_0{}^*}$$

in $\Omega^0(F_{[x]})_{w_0{}^*}$ and defining $i_{w_0{}^*}(\alpha)$ to be $\mathsf{A}(f)_{[w_0{}^*]}$, under the identifications agreed upon above. We define the sheaf $\mathcal{A}$ on $\mathcal{V}_x$ to be the sheaf whose stalk over $w^* \in \mathcal{P}_x{}^{-1}(x^*)$ is $\mathcal{A}_{w^*}$, whose stalk over $y^* \notin \mathcal{P}_x{}^{-1}(x^*)$ is 0, and a basis for whose topology is obtained by admitting the following sections:

(1) If $w_0{}^* \in \mathcal{P}_x{}^{-1}(x^*)$ and f is holomorphic in the neighborhood N of $w_0{}^*$, we admit the section σ defined by $\sigma(w^*) = \mathsf{A}(f)_{[w^*]}$ if $w^* \in N \cap \mathcal{P}_x{}^{-1}(x^*)$, $\sigma(w^*) = 0$ otherwise.

(2) If $y^* \in \mathcal{V}_x - \mathcal{P}_x{}^{-1}(x^*)$ and N is a neighborhood of y^* such that $N \cap \mathcal{P}_x{}^{-1}(x^*)$ is empty, the only possible section of $\mathcal{A}$ over N is the zero section.

If $y^* \notin \mathcal{P}_x{}^{-1}(x^*)$, we define A_{y^*} and i_{y^*} by $\mathsf{A}_{y^*}\colon \Omega^0(F_{[x]})_{y^*} \to \mathcal{A}_{y^*} = 0$ and $i_{y^*}\colon [\Omega^0(F_{[x]}) / \mathfrak{d}\,[\Omega^0(F_{[x]} - k\{m_xS_x{}^*\})]] \to \mathcal{A}_{y^*} = 0$. Thus we obtain the sheaf homomorphism $\mathsf{A}\colon \Omega^0(F_{[x]}) \to \mathcal{A}$ defined by $\mathsf{A}(\alpha) = \mathsf{A}_{y^*}(\alpha)$ if $\alpha \in \Omega^0(F_{[x]})_{y^*}$, while, since the decomposition $f \to \mathsf{A}(f) + \mathsf{B}(f)$ is "analytically continuous" on S_x, i defined by $i(\alpha) = i_{y^*}(\alpha)$ if

$$\alpha \in [\Omega^0(F_{[x]}) / \mathfrak{d}\,[\Omega^0(F_{[x]} - k\{m_xS_x{}^*\})]]_{y^*}$$

is a sheaf isomorphism, $i\colon \Omega^0(F_{[x]})/\mathcal{J}[\Omega^0(F_{[x]}-k\{m_xS_x^*\})] \cong \mathcal{A}$. Therefore we have an isomorphism, $i^*\colon \Gamma(\Omega^0(F_{[x]})/\mathcal{J}[\Omega^0(F_{[x]}-k\{m_xS_x^*\})]) \cong \Gamma(\mathcal{A})$. It is clear that $ij = \mathsf{A}$. Thus we have the "onto" homomorphism, $i^*j^*\colon \Gamma(F_{[x]}) \rightarrow \Gamma(\mathcal{A})$.

We now examine $\Gamma(\mathcal{A})$. Let $\sigma \in \Gamma(\mathcal{A})$. Then under our agreed upon identifications, for each $w \in S_x$, $\sigma(w)$ is a germ in the local ring of holomorphic functions at w invariant under G'_w (actually, if $w^1, \cdots, w^k$ is the complete inverse image of w^* in W_x, $\sigma(w^*)$ prescribes a local holomorphic function f^i at w^i for each i such that if $g \in G_x'$ and $gw^i = w^j$, then $(f^j \circ g)_{[w^i]} = f^i{}_{[w^i]})$. It follows easily from the continuity of σ that there exists a neighborhood M of S_x stable under G_x', and an analytic function f invariant under G_x' on M such that $\mathsf{A}(f)_{[w^*]} = \sigma(w^*)$ if $w \in S_x$. Since f is holomorphic in a neighborhood of S_x in W_x, and since S_x is a compact, complex analytic submanifold of W_x, f is constant on S_x. Therefore if we define $f^*(u) = f(\pi_x^{-1}(u))$ for $u \in \pi_x(M) \subset U_x$, we see by the theorem on removable singularities that f^* is analytic on $\pi_x(M)$ and invariant under G_x. We now examine the power series expansion of f^* at x:

$$f^*(z_x) = \sum a_{m_1\cdots m_n}(z_x^1)^{m_1}\cdots(z_x^n)^{m_n}.$$

It follows from our construction of f and definition of A that $\mathsf{A}(f) = \bar{f}$ at each point $y \in \pi_x^{-1}(x)$. Therefore f^* is a polynomial of degree $< km_x$ invariant under G_x. On the other hand, if we are given an invariant polynomial f^* at x of degree $< km_x$, it is evident that f^* defines naturally a cross-section σ of $\mathcal{A}$ such that f^* is the natural image of σ under the process described above. Hence we have established a natural isomorphism $\lambda\colon \Gamma(\mathcal{A}) \cong I_x(km_x)$, where $I_x(km_x)$ is the module of invariant polynomials at x of degree $< km_x$.

Finally, we point out that there is a natural isomorphism of the holomorphic sections of F with those of $F_{[x]}$. It is obvious, of course, that we have an isomorphism ι of $\Gamma(F)$ *into* $\Gamma(F_{[x]})$. On the other hand, from the facts that $F_{[x]}$ is complex analytically the product bundle over U_l' and that S_x is compact it follows easily, again from the theorem on removable singularities, that ι is onto, $\iota\colon \Gamma(F) \cong \Gamma(F_{[x]})$. Thus we have the homomorphism $\lambda i^*j^*\iota$ of $\Gamma(F)$ onto $I_x(km_x)$, and the kernel of this homomorphism is precisely those cross-sections which, when expressed as holomorphic functions on U_l, have a power series expansion at x containing no terms of degree $< km_x$. Moveover, the image of any element of $\Gamma(F)$ is just the terms of degree $< km_x$ in this power series expansion. (Note that since G_x is linear in $z_x^1, \cdots, z_x^n$, it preserves the degrees of the homogeneous terms.) Thus the existence theorem is proved.

COROLLARY I. *Let* $x^*, y^* \in \mathfrak{V}$, $x^* \neq y^*$. *Let two integers* $h, k > 0$ *be given. In the notation of the preceding section let* F *be a positive bundle on* $\mathfrak{V}$ *such that* $(F_{[x]} - h\{m_x S_x^*\} - k\{m_y S_y^*\} > 0$. *Let* $\{U_x, G_x, v_x\}$ *and* $\{U_y, G_y, v_y\}$ *be* l. u. s.'s *such that* $v_x(x) = x^*$, $v_y(y) = y^*$, *and let* $\{z_x^i\}$ *and* $\{z_y^i\}$ *be coordinates in* U_x *and* U_y *with centers at* x *and* y *respectively. Then there exists a cross-section of* F *which has power series expansions at* x *and* y *with the prescribed invariant terms of degrees* $< hm_x$ *and* $< km_y$ *in* $\{z_x^i\}$ *and* $\{z_y^i\}$ *respectively.*

Letting $h = k = 1$ in Corollary I, we obtain

COROLLARY II. *If* $(F_{[x]} - \{m_x S_x^*\} - \{m_y S_y^*\}) - K_{xy} > 0$, *there exists a pair of cross-sections* σ_1 *and* σ_2 *of* F, σ_1 *non-vanishing at* x *and* y, *such that* $\sigma_2(x)/\sigma_1(x) = 1$ *and* $\sigma_2(y)/\sigma_1(y) = 0$.

7. Imbedding theorems—The main result. Let $\mathfrak{V}$ be a compact, complex analytic V-manifold, and suppose there exist a positive complex line bundle over $\mathfrak{V}$. The purpose of this section is to employ the global methods and results of the preceding section together with some local results of J. P. Serre and H. Cartan [8, 19, 20] in showing how $\mathfrak{V}$ may be naturally regarded as an algebraic variety.

We state some well know definitions. Let $\mathfrak{o}$ be an integral domain contained in the integral domain k and denote by $\mathfrak{o}'$ the integral closure of $\mathfrak{o}$ in k. If $\mathfrak{o} = \mathfrak{o}'$, $\mathfrak{o}$ is said to be integrally closed in k. Let V be a local analytic variety (or, more precisely, a germ of analytic varieties) at the origin of C^n. Then a representative of V is defined as the set of common zeros of some finite number of holomorphic functions in a small neighborhood of the origin. Let $\mathfrak{J}(V)$ be the ideal of V in the ring $\mathfrak{O}^{(n)}$ of local holomorphic functions at the origin. Suppose that V is irreducible, or, equivalently, that $\mathfrak{J}(V)$ is prime; V is said to be (analytically) normal if $\mathfrak{O}^{(n)}/\mathfrak{J}(V)$ is integrally closed in its quotient field. Let $\mathfrak{O}^{(m)}$ be the ring of local holomorphic functions at the origin of C^m and let $f_1, \cdots, f_m$ be elements of $\mathfrak{O}^{(n)}$ which vanish at the origin; then by the ring $\mathfrak{A}(f_1, \cdots, f_m)$ *analytically generated by* $f_1, \cdots, f_m$ we mean the subring of $\mathfrak{O}^{(n)}$ consisting of those $\varphi \in \mathfrak{O}^{(n)}$ such that $\varphi = \phi(f_1, \cdots, f_m)$ in some neighborhood of the origin of C^n, where $\phi \in \mathfrak{O}^{(m)}$ (naturally, ϕ is not necessarily unique).

We now state, in special cases and without proof, two theorems of the 1951-52 Cartan seminar [19] (these are Theorems 5 and 6 of exposé XIV).

We have somewhat specialized the statements of these theorems, as found in the seminar notes, to suit our own particular needs and have labeled them as Theorems A and B.

THEOREM A. *Using the above notation, let* $f_1, \cdots, f_m$ *be functions belonging to* $\mathfrak{O}^{(n)}$ *which vanish at the origin. Moreover, let* $f\colon N \to C^m$ *be the analytic mapping into* C^m *of a small neighborhood* N *of the origin in* C^n *defined by* $f(z) = (f_1(z), \cdots, f_m(z))$. *Then*

(1) *The ideal* $\mathfrak{P}$ *of those* $g \in \mathfrak{O}^{(m)}$ *for which* $g \circ f$ *vanishes in some neighborhood of the origin of* C^n *is prime; and if we denote the variety of* $\mathfrak{P}$ *by* $V(\mathfrak{P})$, *then the germ determined by the point set* $f(N)$ *at the origin is contained in* $V(\mathfrak{P})$.

(2) *If every* $\zeta \in \mathfrak{O}^{(n)}$ *is integral over* $\mathfrak{A}(f_1, \cdots, f_m)$, *then (the germ of)* $f(N) = V(\mathfrak{P})$.

THEOREM B. *Let* $f_1, \cdots, f_m \in \mathfrak{O}^{(n)}$ *and suppose that these functions vanish at the origin. Let* $\mathfrak{A}'$ *be the integral closure of* $\mathfrak{A}(f_1, \cdots, f_m)$ *in* $\mathfrak{O}^{(n)}$. *In order that* $\mathfrak{A}' = \mathfrak{O}^{(n)}$, *it is necessary and sufficient that the origin be an isolated point of the set of common zeros of* $f_1, \cdots, f_m$.

Before stating more local results of Cartan and Serre, we introduce additional notation. Let H be a finite subgroup of the general complex linear group on n variables. We may regard H as a group of automorphisms of $\mathfrak{O}^{(n)}$. Let I be the subring of those elements of $\mathfrak{O}^{(n)}$ which are invariant under H. Then we may summarize the local results which we need in the following two theorems [8, 20] which we state here without proof.

THEOREM C. *There exist a finite number of homogeneous polynomials* $Q_1, \cdots, Q_k \in I$ *such that* $\mathfrak{A}(Q_1, \cdots, Q_k) = I$.

For any $f \in \mathfrak{O}^{(n)}$ let $\omega(f)$ be the degree of the monomials of lowest degree appearing in the power series expansion of f at the origin.

THEOREM D. *Let* $Q_1, \cdots, Q_k$ *be homogeneous polynomials belonging to* I *such that* $\mathfrak{A}(Q_1, \cdots, Q_k) = I$. *Let* $d = \max_i(\deg Q_i)$. *Let* $f_1, \cdots, f_k$ *be elements of* I *such that* $\omega(Q_i - f_i) > d$, $i = 1, \cdots, k$. *Then* $\mathfrak{A}(f_1, \cdots, f_k) = I$.

Of all systems $Q_1, \cdots, Q_k$ as in Theorem D there is one for which $d = \max_i(\deg Q_i)$ is least; we denote this least value of d by $d(H)$.

Let $f_1, \cdots, f_m$ be elements of I vanishing at the origin such that $\mathfrak{A}(f_1, \cdots, f_m) = I$. We adopt all the notations of Theorem A. Then it follows from our previous considerations and from Theorem A that $f(N)$ is an analytic variety V at the origin of C^m. Let $\mathfrak{R}$ be the local ring $\mathfrak{O}^{(m)}/\mathfrak{P}$ of V. We will establish a natural isomorphism $\mathfrak{i}\colon I \cong \mathfrak{R}$. Let $\varphi \in I$. Then $\varphi = \phi(f_1, \cdots, f_m)$, where $\phi \in \mathfrak{O}^{(m)}$. We let $\mathfrak{i}(\varphi)$ be the coset to which ϕ belongs in $\mathfrak{O}^{(m)}/\mathfrak{P}$. $\mathfrak{i}$ is well-defined, for if $\phi(f_1, \cdots, f_m) = \phi'(f_1, \cdots, f_m)$, $\phi - \phi'$ vanishes on V, and therefore $\phi - \phi' \in \mathfrak{P}$. It is a trivial exercise to show that $\mathfrak{i}$ is in fact a homomorphism with kernel zero and that $\mathfrak{i}(I) = \mathfrak{R}$. Since I is clearly integrally closed in its quotient field, it follows that V is (analytically) normal at the origin (of C^m).

For any $\varphi \in \mathfrak{O}^{(n)}$, we let $P_H(\varphi)$ denote the polynomial of degree $d(H)$ such that $\omega(\varphi - P_H(\varphi)) > d(H)$. Suppose that $f_1, \cdots, f_m$ are elements of I vanishing at the origin such that $P_H(f_1), \cdots, P_H(f_m)$ span the complex module of polynomials of degree $\leqq d(H)$ belonging to I which vanish at the origin. Then clearly (Theorem D) $\mathfrak{A}(f_1, \cdots, f_m) = I$. Hence in the above notation we have

LOCAL IMBEDDING THEOREM. *Let H be a finite subgroup of the general complex linear group in n variables. Let $\mathfrak{O}^{(n)}$ be the ring of holomorphic functions at the origin of C^n, and let I be the maximal subring of $\mathfrak{O}^{(n)}$ elementwise invariant under H. If $f_1, \cdots, f_m$ are elements of I vanishing at the origin such that $P_H(f_1), \cdots, P_H(f_m)$ and 1 span the complex module of polynomials in I of degree $\leqq d(H)$, then the mapping f defined by $f(z) = (f_1(z), \cdots, f_m(z))$ maps a small neighborhood of the origin of C^n onto an analytic variety V which is irreducible and (analytically) normal at the origin of C^m, and, moreover, $I \cong \mathfrak{O}^{(m)}/\mathfrak{P}(V)$.*

Let $\mathfrak{V}$ be an n-dimensional V-manifold and let Φ be a complex analytic mapping of $\mathfrak{V}$ into an m-dimensional complex analytic manifold M. Let $x^* \in \mathfrak{V}$, let $\{U, G, v\}$ be a l.u.s. such that $v(x) = x^*$ and such that the coordinates $z^1, \cdots, z^n$ on U have center at x, and let $\zeta^1, \cdots, \zeta^m$ be local coordinates with center at $y = \Phi(x^*)$ on M. Denote by Φ' the map thus induced by Φ of a small neighborhood N of x into a small neighborhood of the origin in C^m: $\Phi'(z) = \Phi'(z^1, \cdots, z^n) = (\zeta^1, \cdots, \zeta^m)$, where $\zeta^i = f_i(z)$, $i = 1, \cdots, m, f_1, \cdots, f_m$ being invariant under G_x. Then we say that Φ is biregular at x^* if $f_1, \cdots, f_m$ analytically generate the whole local ring I of holomorphic functions invariant under G_x. It follows immediately from the local imbedding theorem that if Φ is biregular at x^* and if U is a small neighborhood of x^*, then $\Phi(U)$ is normal at y, the local ring of $\Phi(U)$ at y is naturally isomorphic to I, and if G_x consists of the identity alone, then Φ is biregular at x in the usual sense (note that in this case a small neighborhood of x is an ordinary complex analytic manifold). Since I is isomorphic to the ring of local holomorphic functions on $\mathcal{V}$ at x^*, the latter is isomorphic to the local ring of $\Phi(U)$ at $\Phi(x^*)$. A sufficient condition for Φ to be biregular at x^* is that $P_{G_x}(f_1), \cdots, P_{G_x}(f_m)$ and 1 span the complex module of polynomials invariant under G_x of degrees $\leqq d(G_x)$.

We now state and prove the theorem which has been the main object of this paper.

Global Imbedding Theorem. *Let $\mathcal{V}$ be a compact, n-dimensional, complex analytic V-manifold. Suppose there exists a positive complex line bundle over $\mathcal{V}$. Then $\mathcal{V}$ is an algebraic variety. More precisely, there exists a homeomorphism Φ of $\mathcal{V}$ into a complex projective space $\mathfrak{S}^m$ such that Φ is biregular at every point of $\mathcal{V}$ and $\Phi(\mathcal{V})$ is an algebraic variety in $\mathfrak{S}^m$. The mapping Φ is obtained in terms of a basis of holomorphic cross-sections of a sufficiently positive absolute complex line bundle in a manner to be described in the proof.*

Proof. Let $x_0^1, \cdots, x_0^p$ and $U^*(x_0^i)$, $i = 1, \cdots, p$, be chosen as in Auxiliary Theorem I of Section 5 and choose positive integers k_i, $i = 1, \cdots, p$, as follows. Let $\{U^i, G^i, v^i\}$ be a l. u. s. such that $U^*(x_0^i) \subset U^i$, let $G^i{}_1 = G^i$, $G^i{}_2$, $\cdots, G^i{}_{n_i}$ be the subgroups of G^i, and let $k_i > \max_j(d(G^i{}_j))$. Then by Auxiliary Theorems I and II of Section 5, there exists a positive, absolute, complex line bundle F on $\mathcal{V}$ such that

(I) $(F_{[x]} - k_i\{m_x S_x{}^*\}) - K_x > 0$, $i = 1, \cdots, p$, and

(II) $(F_{[x]} - \{m_x S_x{}^*\} - \{m_y S_y{}^*\}) - K_{xy} > 0$ for all $x^*, y^* \in \mathcal{V}$, $x^* \neq y^*$.

By Theorem F of [2], $\Gamma(F)$ is finite dimensional. Let $\sigma_0, \cdots, \sigma_m$ be a basis for $\Gamma(F)$. Since (II) is satisfied, it follows from Corollary II of Section 6 that for each $x^* \in \mathcal{V}$ at least one $\sigma_i(x^*) \neq 0$.

Let x^* belong to the coordinate neighborhhod V_k (on $\mathcal{V}$) of the (absolute) bundle F and let $\sigma_{0k}, \cdots, \sigma_{mk}$ be the holomorphic functions which represent $\sigma_0, \cdots, \sigma_m$ in V_k. The ratios $\sigma_{ik}(x^*)/\sigma_{jk}(x^*)$ (defined for all j such that $\sigma_{jk}(x^*) \neq 0$) are evidently independent of the choice of coordinate neighborhood V_k. Therefore, the mapping $\Phi\colon \mathcal{V} \rightarrow \mathfrak{S}^m$ defined by $\Phi(x^*) = (\sigma_{0k}(x^*), \cdots, \sigma_{mk}(x^*))$, if $x^* \in V_k$, is everywhere defined and continuous. By Corollary II of Section 6, Φ is one-to-one. Since $\mathcal{V}$ is compact, Φ is a homeomorphism of $\mathcal{V}$ onto $\Phi(\mathcal{V})$.

Let x^* be a point of $\mathcal{V}$ and let $\{U, G, v\}$ be a l. u. s. such that $v(x) = x^*$, such that the coordinates $z^1, \cdots, z^n$ in U have center at x, and such that $v(U)$ is contained in a single coordinate neighborhood V_k for F. By an appropriate linear transformation on $\sigma_0, \cdots, \sigma_m$, we obtain a new basis $\sigma_0', \cdots, \sigma_m'$ for $\Gamma(F)$ such that $P_G(\sigma_0') = 1$ and $\sigma_i(x^*) = 0$ if $i > 1$; then it is clear from (I) and the Basic Existence Theorem of Section 6 that $\Lambda(\sigma_{1k}'/\sigma_{0k}', \cdots, \sigma_{mk}'/\sigma_{0k}') = I$, and therefore Φ is biregular at x^* since the above linear transformation on $\sigma_0, \cdots, \sigma_m$ amounts simply to a non-singular transformation of coordinates at $\Phi(x^*)$.

Our Local Imbedding Theorem shows that $\Phi(\mathcal{V})$ is a complex analytic subvariety of $\mathfrak{S}^m$, and, being compact, it is an algebraic variety by Chow's Theorem [9, 12, 20]. q. e. d.

It is easy to see that if Φ_1 is another projective imbedding of $\mathcal{V}$ constructed as above, then the two projective models $\Phi(\mathcal{V})$ and $\Phi_1(\mathcal{V})$ of $\mathcal{V}$ are biregularly equivalent.

We list some applications of the theorem just proved. Let $\mathcal{D}$, as in Section 3, be a bounded domain in C^n and let G be a discontinuous group of complex analytic transformations of $\mathcal{D}$ such that $\mathcal{D}/G$ is compact (see [4, 22]). Then $\mathcal{D}/G$ is a compact, complex analytic V-manifold, and, as we see from Section 3, the Bergman metric affords a positive definite form in the characteristic class of the positive complex line bundle K whose holomorphic cross-sections are to be naturally identified with the automorphic forms of weight 1. Then there is a multiple m_0K of K such that for all sufficiently large positive integers N, a basis of holomorphic cross-sections of Nm_0K (i. e., automorphic forms of weight Nm_0) affords an imbedding Φ of $\mathcal{D}/G$ into a projective space $\mathfrak{S}^m$ such that Φ satisfies the conditions of our main theorem. In other words, if $\theta_0, \cdots, \theta_m$ are a basis of the module of automorphic forms of weight Nm_0, the map $\Phi' \colon \mathcal{D} \to \mathfrak{S}^m$, defined by $\Phi'(x) = (\theta_0(x), \cdots, \theta_m(x))$, is an imbedding of $\mathcal{D}$ into $\mathfrak{S}^m$ such that $\Phi'(\mathcal{D})$ is an algebraic variety, and such that Φ' may be factored by way of $\mathcal{D}/G$:

$$\begin{tikzcd}
& \mathcal{D}/G \arrow[dr, "\Phi"] & \\
\mathcal{D} \arrow[ur, "\Theta"] \arrow[rr, "\Phi'"'] & & \Phi(\mathcal{D}/G) \subset \mathfrak{S}^m
\end{tikzcd}$$

where Φ is a homeomorphism and $\Phi' = \Phi \circ \Theta$. This result has already been obtained in the Cartan seminar of 1953-54 together with the additional information that, a priori, we only need require $\theta_0, \cdots, \theta_m$ to be a basis for the Poincaré θ-series of weight Nm_0. That proof is based on the kind of local imbedding theorem given above and on the elementary properties of θ-series. It is nearly obvious that if we let $\{P_\alpha\}$ be the set of homogeneous polynomials in $m+1$ variables such that $P_\alpha(\theta_0,\cdots,\theta_m)\equiv 0$ in $\mathfrak{D}$, then $\Phi'(\mathfrak{D})$ is the variety in $\mathfrak{S}^m$ defined by the equations $P_\alpha(t^0,\cdots,t^m)=0$ in the homogeneous coordinates $t^0,\cdots,t^m$.

Another example is obtained by letting X be a non-singular algebraic variety in the complex projective space $\mathfrak{S}^s$ and letting G be a finite group of complex transformations of X.[5] Then X/G is a compact, complex analytic V-manifold and a positive complex line bundle is constructed as follows:

Let S be a general non-singular hyperplane section of X. Then GS (the union of the translates of S under G) evidently gives rise to an absolute divisor S^G on X/G, and the bundle $\{S^G\}$ is positive since $\{S\}$ is a positive bundle on X, the characteristic class of $\{S\}$ being simply the class of the metric form ω induced on X by the "standard" metric of $\mathfrak{S}^s$, and a form in the characteristic class of S^G being induced by the sum of the translates of ω under G. If $X=\mathfrak{S}^s$, the imbedding is given by a basis of invariant homogeneous polynomials of a sufficiently high degree.

A third example of a V-manifold has been described by Satake, in a recent article [18], in compactifying the fundamental domain of the 2-dimensional modular group of Siegel which acts in the space of 2×2 complex symmetric matrices of positive definite imaginary part. The author of the present article has shown that there exists a positive definite bundle over this V-manifold, which is consequently an algebraic variety.

There are, of course, compact, complex analytic V-manifolds which are not algebraic—an example of such is afforded by every compact, complex analytic manifold (in the usual sense) which is not algebraic.

PRINCETON UNIVERSITY.

REFERENCES.

[1] W. L. Baily, "On the quotient of an analytic manifold . . .," *Proceedings of the National Academy of Sciences, U. S. A.*, vol. 40 (1954), pp. 804-808.

[2] ———, "The decomposition theorem for V-manifolds," *American Journal of Mathematics*, vol. 78 (1956), pp. 862-888.

[3] S. Bergman, "Sur la fonction noyau d'un domaine et ses applicagions dans la theorie des transformations pseudo-conformes," *Memorial des Sciences Mathematiques*, vol. 108, Paris, 1948.

---

[5] P. E. Conner has recently obtained a formula for the Euler-Poincaré characteristic of the space X/G. See [10].

[4] S. Bochner, "Algebraic and linear dependence of automorphic functions in several variables," *Journal of the Indian Mathematical Society*, vol. 16 (1952), pp. 1-6.

[5] ———, "Curvature and Betti numbers" I and II, *Annals of Mathematics*, vol. 49 (1948), pp. 379-390; vol. 50 (1949), pp. 77-93.

[6] S. Bochner and W. T. Martin, *Several Complex Variables*, Princeton University Press, Princeton, 1948.

[7] A. Borel, "Les fonctions automorphes de plusieurs variables complexes," *Bulletin de la Société Mathématique de France*, vol. 80 (1952), pp. 167-182

[8] H. Cartan, "Quotient d'un espace analytique par un group d'automorphisms," *Algebraic Geometry and Topology: A Symposium in Honor of S. Lefschetz*, Princeton University Press, Princeton, 1957.

[9] W. L. Chow, "On compact complex analytic varieties," *American Journal of Mathematics*, vol. 71 (1949), pp. 893-914.

[10] P. E. Conner, "Concerning the action of a finite group," *Proceedings of the National Academy of Sciences, U. S. A.*, vol. 42 (1956), pp. 349-351.

[11] P. Dolbeault, "Sur la cohomologie des varietes analytiques complexes," *Comptes Rendus, Academie des Sciences*, vol. 236 (1953), pp. 175-177.

[12] H. Kneser, "Analytische Mannigfaltigkeiten im komplexen Projektiven Raum," *Mathematische Nachrichten*, vol. 4 (1951), pp. 382-391.

[13] K. Kodaira, "On cohomology groups of compact analytic varieties with coefficients in some analytic faisceaux," *Proceedings of the National Academy of Sciences, U. S. A.*, vol. 39 (1953), pp. 865-868.

[14] ———, "On a differential geometric method in the theory of analytic stacks," *Proceedings of the National Academy of Sciences, U. S. A.*, vol. 39 (1953), pp. 1268-1273.

[15] ———, "On Kähler varieties of restricted type (An intrinsic characterization of algebraic varieties)," *Annals of Mathematics*, vol. 60 (1954), pp. 28-48.

[16] K. Kodaira and D. C. Spencer, "Groups of complex line bundles over compact Kähler varieties," *Proceedings of the National Academy of Sciences, U. S. A.*, vol. 39 (1953), pp. 868-872.

[17] I. Satake, "On a generalization of the notion of manifold," *Proceedings of the National Academy of Sciences, U. S. A.*, vol. 42 (1956).

[18] ———, "On Siegel's modular functions," *Proceedings of the International Symposium on Algebraic Number Theory*, Toyko-Nikko, 1955.

[19] Seminaire de H. Cartan, 1951-1952 (hectographed notes).

[20] Seminaire E. N. S., 1953-1954 (hectographed notes).

[21] Sheaves (mimeographed notes of a seminar), Princeton, 1953-1954.

[22] C. L. Siegel, *Analytic Functions of Several Complex Variables*, Institute for Advanced Study, Princeton, 1948-1949, pp. 124 ff.

[23] N. E. Steenrod, *The Topology of Fibre Bundles*, Princeton University Press, Princeton, 1951.

[24] A. Weil, "Sur les theoremes de deRham," *Commentarii Mathematici Helvetici*, vol. 26 (1952), pp. 119-145.

ON ESTIMATING ELLIPTIC PARTIAL DIFFERENTIAL OPERATORS IN THE L_2 NORM.*

By MARTIN SCHECHTER.[1]

1. Introduction. In recent years many authors have been treating problems in partial differential equations within the framework of Hilbert spaces involving L_2 norms. As should be expected, it is necessary to establish so called *a priori* estimates. In particular, if A is a linear m-th order partial differential operator with continuous coefficients and D^m denotes the generic m-th order derivative, it is desired to know when one has

$$\| D^m u \|^2 \leqq K(\| Au \|^2 + \| u \|^2) \tag{1}$$

for all functions u in a given class U.[2] (The functions u as well as the coefficients of A are to be complex valued and defined in the closure of a domain G. The norm is that of $L_2(G)$.)

If U is the set of infinitely differentiable functions with compact support in G, it is easily shown that ellipticity is a necessary and sufficient condition for (1) to hold.[3] On the other hand, if no boundary restrictions are placed on the u, the inequality is violated (cf. [1]).

However, as suggested by the Dirichlet problem, one can consider intermediate classes of functions, namely functions having derivatives up to a certain order vanish on the boundary. In this connection, Guseva [7], Nirenberg [6], and Browder [2] proved that (1) holds for operators of even order with real parts elliptic and for functions u having zero Dirichlet data, i.e., functions which vanish on the boundary together with all derivatives of order less than $m/2$.

It is the purpose of this paper to study the intermediate cases more fully. Let n be the dimension of G and let $C^r(G)$ be the set of functions infinitely differentiable in $\bar{G}$ having all derivatives of order less than r vanish

---

* Received December 17, 1956.

[1] This work was completed while the author was an Institute of Mathematical Sciences Fellow at New York University.

[2] The letter K will denote a constant independent of the functions u. It will denote a different constant in different expressions.

[3] See Lemma 9 of Section 6, this paper. Note that our definition of ellipticity (Section 2) is weaker than that of some authors (cf. [4]).

on the boundary. (If $r > 0$, it is understood that the functions themselves vanish on the boundary.) It is convenient to consider the case $n = 2$ separately. In all other cases we have the simple result: (1) holds for all $u \in C^r(G)$ if and only if A is elliptic and $m \leqq 2r$. (Precise regularity conditions assumed for the boundary of G are given in Section 6.) Moreover, if the coefficients of A are real, this result holds also for $n = 2$.

In the general case of $n = 2$ we must take into consideration the roots of the characteristic polynomial P of A. Properly defined (see Section 2) there are, at the boundary, exactly m roots of P with imaginary parts perpendicular to the boundary. Let p_1 represent the number of those with imaginary parts directed inward and p_2 the number having imaginary parts directed outward. Setting $q = \max(p_1, p_2)$ we have for $n = 2$: (1) holds for all $u \in C^r(G)$ if and only if A is elliptic and $q \leqq r$. (The reason for the simpler formulation for higher n is that in those cases ellipticity implies that m is even and that $q = m/2$. See Section 2.)

In the next section we make the necessary definitions and state our main results (Theorems 1 and 2). In proving them (Section 6) we employ a method developed by Gårding [4] and Aronszajn [1]. It consists of breaking G up into small subdomains and, after appropriate transformations, of approximating A by a homogeneous operator A' with constant coefficients. This reduces the problem to a similar one for A' in a special type of domain. The corresponding theorems for A' are stated in Section 3 and proved in Section 5 by means of Fourier transform methods introduced in Section 4.

For the special case of the Laplacian operator, inequality (1) was first proved by Ladyženskaya and Michelin for functions having zero Dirichlet data on the boundary (cf. [7]).

Aronszajn, in an unpublished work, has treated inequalities of the form (1) in which $\| Au \|^2$ is replaced by a general bilinear form. He considered functions with no boundary restrictions.

S. Agmon, A. Douglis, and L. Nirenberg have proved inequality (1) for functions satisfying very general mixed initial values and boundary conditions. Their work is as yet unpublished.

The author would like to express his sincerest gratitude to Professor Louis Nirenberg, who suggested the problem, for his invaluable assistance and expert guidance.

2. Statement of results.

Let G be a bounded n dimensional domain with closure $\bar{G}$ and boundary B. We assume, for convenience, that B is infinitely differentiable, although this is not necessary.[4] By $C^r(G)$ we shall denote the class of all infinitely differentiable complex valued functions defined in $\bar{G}$ and having all derivatives of order less than r vanish on B.

Let $\mu = (\mu_1, \mu_2, \cdots, \mu_n)$ be a sequence of indices, each $\geqq 0$, and set $|\mu| = \sum \mu_k$. If $\xi = (\xi_1, \xi_2, \cdots, \xi_n)$ is an n dimensional vector, we employ the notation $\xi^\mu = \xi_1^{\mu_1} \xi_2^{\mu_2} \cdots \xi_n^{\mu_n}$. Similarly, if $x = (x_1, x_2, \cdots, x_n)$ is a coordinate system in G, set

$$D_k = -i\partial/\partial x_k, \qquad D^\mu = D_1^{\mu_1} D_2^{\mu_2} \cdots D_n^{\mu_n}.$$

We shall use the following norms:

$$\| u \|^2 = \int_G | u | \, dx, \qquad (| u |_m)^2 = \sum_{|\mu|=m} \| D^\mu u \|^2, \qquad (\| u \|_m)^2 = \sum_{t \leqq m} | u |_t^2.$$

Suppose that a_μ are complex valued functions continuous in $\bar{G}$. We consider operators of the form $A = \sum a_\mu D^\mu$, where $|\mu| \leqq m$, and shall call A elliptic in $\bar{G}$ if its characteristic polynomial $P(x, \xi) = \sum a_\mu \xi^\mu$, where $|\mu| = m$, does not vanish for real vectors $\xi \neq 0$ at any point of $\bar{G}$. We are now in a position to state our first result.

THEOREM 1. *If $n > 2$, a necessary and sufficient condition that*

$$\text{(I)} \qquad \| u \|_m^2 \leqq K(\| Au \|^2 + \| u \|^2) \quad \textit{for all } u \in C^r(G)$$

is that A is elliptic and $m \leqq 2r$.

In proving Theorem 1 we take into account the following considerations. At each point of B we have exactly m complex vector roots of P having imaginary parts perpendicular to B. They are to be found as follows: Rotate the coordinate axes until x_n is perpendicular to B at the given point. A and P are correspondingly changed. Now let $\xi_1, \xi_2, \cdots, \xi_{n-1}$ take on any real values not all zero. Then there will be m complex roots of P for ξ_n. Let p_1 be the number of those roots having positive imaginary parts and let p_2 be the number with negative imaginary parts. If A is elliptic, these quantities do not change as $\xi_1, \xi_2, \cdots, \xi_{n-1}$ are allowed to take on all real values not all zero. Moreover, continuity of the coefficients together with ellipticity will guarantee that p_1 and p_2 remain unchanged as one moves along B. Hence, for elliptic operators, the quantity $q = \max(p_1, p_2)$ is properly defined. Theorem 1 now follows from the more general

THEOREM 2. (I) *holds if and only if A is elliptic and $q \leqq r$.*

---

[4] Weaker conditions on B which are sufficient for the validity of the theorems stated here are discussed in Section 6.

COROLLARY 1. (I) *holds if* $m \leqq 2r$ *and there is a complex constant* γ *such that* $\operatorname{Re} \gamma A$ *is elliptic.*

The connection between the two theorems is seen in the

Remark. If $n > 2$, the ellipticity of A implies that m is even and that $q = m/2$.

Proof. If $n > 2$, one can continuously take the vector $(\xi_1, \xi_2, \cdots, \xi_{n-1})$ through real values into the vector $(-\xi_1, -\xi_2, \cdots, -\xi_{n-1})$ without going through the origin. By our previous argument the quantities p_1 and p_2 remain unchanged. But the signs of the corresponding roots will be reversed. Hence $p_1 = p_2$.

In the two dimensional case, q can have other values and Theorem 2 is needed. However, if the coefficients of A are real, $p_1 = p_2$ and Theorem 1 holds also for $n = 2$.

Theorems 1 and 2 will be proved in Section 6 by means of the special theorems of the next section.

3. Operators with constant coefficients.

We now consider theorems similar to those of Section 2 but applying to a special type of domain and to homogeneous operators with constant coefficients.

Let G^* be an n dimensional domain having part of its boundary on the hyperplane $x_n = 0$. Denote this part by B^*_1 and the remainded by B^*_2. By $C^{*r}(G^*)$ we shall mean the class of functions u satisfying

1) u is infinitely differentiable in $\bar{G}^*$;
2) u vanishes near B^*_2;
3) all derivatives of u of order $< r$ vanish on B^*_1.

We consider an m-th order homogeneous operator with constant (complex) coefficients $A = \sum a_\mu D^\mu$, where $|\mu| = m$. If A is elliptic, its characteristic polynomial $P(\xi) = \sum a_\mu \xi^\mu$, where $|\mu| = m$, does not vanish for any real vector $\xi \neq 0$.

Corresponding to Theorem 1, we have

THEOREM 3. *For* $n > 2$,

$$\text{(II)} \qquad |u|_m \leqq K \, \|Au\| \quad \text{for all } u \in C^{*r}(G^*)$$

if and only if A *is elliptic and* $m \leqq 2r$.

The quantities p_1, p_2, q for A are introduced as follows: Let $\xi_1, \xi_2, \cdots, \xi_{n-1}$

take on any set of real values not all zero. There will be m complex roots of P for ξ_n. Let p_1 be the number of those with positive imaginary parts and p_2 the number with negative imaginary parts. Set $q = \max(p_1, p_2)$.

THEOREM 4. (II) *holds if and only if* A *is elliptic and* $q \leqq r$.

COROLLARY 2. (II) *holds if* $m \leqq 2r$ *and there is a complex constant* γ *such that* $\operatorname{Re} \gamma A$ *is elliptic.*

The proofs of these results will be given in Section 5.

4. Preliminaries.

In this and the following section, we shall alter our notation slightly in order to facilitate the proofs. Set

$$x = (x_1, x_2, \cdots, x_{n-1}), \quad y = x_n; \qquad \xi = (\xi_1, \xi_2, \cdots, \xi_{n-1}), \quad \eta = \xi_n;$$

$$\mu = (\mu_1, \mu_2, \cdots, \mu_{n-1}); \qquad \xi x = \xi_1 x_1 + \xi_2 x_2 + \cdots + \xi_{n-1} x_{n-1}.$$

We make use of the Fourier transform

$$u^* = (2\pi)^{-n/2} \int \exp - i(\xi x + \eta y) u(x, y)\, dx dy,$$

applied to functions $u \in C^{*r}(G^*)$. (Whenever limits are omitted, integration is to be taken over all space. We assume $u \equiv 0$ outside G^*.)

By partial integration we have

$$(2) \qquad (D^\mu u)^* = \xi^\mu u^*, \qquad (D_n u)^* = \eta u^* + u',$$

where $u' = -i(2\pi)^{-n/2} \int \exp(-i\xi x) u(x, 0)\, dx$. Hence, by induction,

$$(3) \qquad (D_n^k u)^* = \eta^k u^* + \sum_{s=r}^{k-1} \eta^{k-s-1} (D_n^s u)'.$$

LEMMA 1. *If* $u \in C^{*1}(G^*)$, *then* $\int u^* d\eta = 0$.

Proof. For $v(y)$ continuous, piecewise smooth, and in $L_1(-\infty, \infty)$,

$$v(z) = \frac{1}{2\pi} \int \exp(i\eta z) \int \exp(-i\eta y) v(y)\, dy d\eta.$$

Set $z = 0$ and $v(y) = \frac{1}{2\pi} \int \exp(-i\xi x) u(x, y)\, dx$.

LEMMA 2. *If* $u \in C^{*r}(G^*)$, *then* $\int \eta^s u^* d\eta = 0$ *for* $0 \leqq s < r$.

Proof. Since $(D_n^s u) \in C^{*1}(G^*)$, we have by Lemma 1, $\int (D_n^s u)^* d\eta = 0$. But $(D_n^s u)^* = \eta^s u^*$.

LEMMA 3. *If* $H(\xi, \eta)$ *is homogeneous of degree* t *in* (ξ, η), *then* $F(\xi) = \int H(\xi, \eta)\, d\eta$ *(provided it exists) is homogeneous of degree* $t + 1$ *in* ξ.

Proof. If $\lambda > 0$, set $\eta' = \eta/\lambda$. Then

$$F(\lambda\xi) = \int H(\lambda\xi, \eta)\, d\eta = \int H(\lambda\xi, \lambda\eta')\, d\lambda\eta' = \lambda^{t+1} \int H(\xi, \eta')\, d\eta' = \lambda^{t+1} F(\xi).$$

Consider a homogeneous m-th order operator with constant coefficients $A = \sum a_\mu D^\mu D_n{}^k$ and its characteristic polynomial $P(\xi, \eta) = \sum a_\mu \xi^\mu \eta^k$, where $|\mu| + k = m$. If $u \in C^{*r}(G^*)$, we have, by (2) and (3), $(Au)^* = Pu^* + S$, where $S = \sum_{t=1}^{m-r} g_t \eta^{t-1}$ and, if $|\xi|^2 = \sum_{j=1}^{n-1} |\xi_j|^2$ and $\xi \neq 0$,

$$g_t(\xi) = \sum_{k=t+r}^{m} w_{k-t} |\xi|^{k-t-1} \sum_{|\mu|+k=m} a_\mu \xi^\mu, \qquad 1 \leqq t \leqq m - r$$

$$w_s(\xi) = |\xi|^{-s-1}(D_n{}^s u)' \text{ if } \xi \neq 0,\ w_s(\xi) = 0 \text{ if } \xi = 0 \qquad r \leqq s < m.$$

LEMMA 4. *If* $a_{00\cdots 0} \neq 0$, *then* $g_t(\xi_0) = 0$ for $1 \leqq t \leqq m - r$ *if and only if* $w_s(\xi_0) = 0$ *for* $r \leqq s < m$.

Proof. Start with $t = m - r$.

LEMMA 5 (Aronszajn). *Let* A *be an elliptic operator and assume that for* $\xi \neq 0$ *and* $u \in C^{*r}(G^*)$,

$$\int |(Au)^*|^2\, d\eta = \int |Pu^* + M|^2\, d\eta + \sum H_{st} w_s \bar{w}_t,$$

where

a) $M = \sum V_s w_s$ *and each* V_s *is homogeneous of degree* m *in* (ξ, η);

b) *Each* H_{st} *is homogeneous in* ξ *of degree* $2m + 1$;

c) *For each real* $\xi \neq 0$, *the matrix* (H_{st}) *is positive definite.*

Conclusion. (II) *holds.*

Proof. Let $D^m u$ be any m-th order derivative of u. Then by (2) and (3), $(D^m u)^* = Qu^* + T$, where Q is an m-th power of (ξ, η) and T is analogous to S. Setting $J = |P|^2 - \epsilon |Q|^2$, we have

$$\begin{aligned}\int (|(Au)^*|^2 - \epsilon |(D^m u)^*|^2)\, d\eta &= \sum H_{st} w_s \bar{w}_t \\ &\quad + \int (J |u^*|^2 + 2\mathrm{Re}\, u^*(P\bar{M} - \epsilon Q\bar{T}) + |M|^2 - \epsilon |T|^2)\, d\eta \\ &= \sum H_{st} w_s \bar{w}_t + \int J |u^* + J^{-1}(\bar{P}M - \epsilon \bar{Q}T)|^2\, d\eta \\ &\quad + \int J^{-1}(J(|M|^2 - \epsilon |T|^2) - |\bar{P}M - \epsilon \bar{Q}T|^2)\, d\eta.\end{aligned}$$

Since A is elliptic, we can take ϵ so small that $J \geqq 0$. Moreover, T has the same homogeneity properties as M. Hence

$$\int (|(Au)^*|^2 - \epsilon |(D^m u)^*|^2)\, d\eta \geqq \sum H_{st} w_s \bar{w}_t - \epsilon \sum L_{st} w_s \bar{w}_t,$$

where the L_{st}, by Lemma 3, are homogeneous in ξ of degree $2m+1$. Now consider

$$\phi(\xi, w) = (\sum L_{st} w_s \bar{w}_t)/(\sum H_{st} w_s \bar{w}_t),$$

where $w = (w_r, w_{r+1}, \cdots, w_{m-1})$. Since $\phi(\lambda\xi, w) = \phi(\xi, \lambda w) = \phi(\xi, w)$ for all $\lambda > 0$, we may consider ϕ defined only on the compact set $|\xi| = |w| = 1$. Since, by hypothesis, the denominator does not vanish on this set and all functions are continuous, there is a constant K such that $\phi(\xi, w) < K$ for all ξ, w. Taking $\epsilon < K^{-1}$ we have

$$\int (|(Au)^*|^2 - \epsilon |(D^m u)^*|^2) d\eta \geqq 0 \text{ for all } \xi \neq 0.$$

Hence, by the Parseval identity,

$$\int (|Au|^2 - \epsilon |D^m u|^2) dx dy = \int (|(Au)^*|^2 - \epsilon |(D^m u)^*|^2) d\xi d\eta \geqq 0.$$

Q. e. d.

LEMMA 6. *Let $P(z)$ be a polynomial of degree $\geqq 2q$ having exactly q roots in the half plane* $\operatorname{Im} z > 0$ *and no real roots. If*

$$c_{st} = \int_{-\infty}^{\infty} x^{s+t}/P(x)\, dx \qquad 0 \leqq s, t < q,$$

then the $q \times q$ matrix (c_{st}) is non-singular.

Proof.[5] Set $P = P_1 P_2$, where P_1 contains only the q roots with positive imaginary parts. Suppose that

$$\sum_{t=0}^{q-1} c_{st} \lambda_t = 0 \tag{4}$$

and not all the complex numbers λ_t vanish. We can extend the integrals to be complex line integrals along a path E enclosing the q roots. Hence by (4),

$$\int_E z^s Q(z)/P(z)\, dz = 0 \qquad 0 \leqq s < q, \tag{5}$$

where $Q(z) = \sum_{t=0}^{q-1} \lambda_t z^t$. We may assume P_1 and Q relatively prime. Otherwise, the common factor can be cancelled in (5) and the resulting polynomials used. Thus there are polynomials F_1, H_1 such that $F_1 Q + H_1 P_1 = 1$, and hence there are polynomials F, H such that $FQ + HP_1 = z^{q-1} P_2$. By dividing

---

[5] This proof was suggested by Shmuel Agmon. It replaces the cumbersome one originally intended by the author.

F by P_1 and taking the remainder if necessary, we can demand that the degree of F be less than q. Now

$$\int_E F(z)Q(z)/P(z)dz = \int_E (FQ + HP_1)/P\, dz = \int_E z^{q-1}/P_1\, dz \neq 0.$$

But this contradicts (5). Hence all the λ_t vanish. Q. e. d.

Lemmas 1-6 are used in the next section to prove Theorem 4.

5. Proof of Theorem 4. Let G be any domain, and denote by $U(G)$ the class of infinitely differentiable functions with compact support in G. If A is any m-th order operator with constant coefficients, we have

LEMMA 7 (Gårding). *The inequality*

$$\text{(III)} \qquad \| u \|_m^2 \leqq K(\| Au \|^2 + \| u \|^2) \quad \textit{for all } u \in U(G)$$

holds if and only if A is elliptic.

Sufficiency may be proved by applying Fourier transfroms and the Parseval identity (cf. [4]). Necessity may be obtained either by a counter example [1] or a device due to Hörmander [5].

Proof of Theorem 4. *Sufficiency.* Suppose that $u \in C^{*r}(G^*)$ and let w be defined as in Section 4. Set

$$h_t(\xi) = \sum V_{st}\bar{w}_s, \qquad R = \sum_{t=1}^{m-q} h_t \eta^{t-1},$$

where each V_{st} is homogeneous in ξ of degree $2m - t + 1$. Since $m - q \leqq q \leqq r$, we have, by Lemma 2, $\int u^* R d\eta = 0$. Using the notation of Section 4, we have

$$\begin{aligned} \int |(Au)^*|^2 d\eta &= \int (|Pu^*|^2 + 2\mathrm{Re}\, u^*(P\bar{S} - cR) + |S|^2) d\eta \\ &= \int |Pu^* + \bar{P}^{-1}(\bar{P}S - c\bar{R})|^2 d\eta + \int |P|^{-2}(|PS|^2 - |\bar{P}S - c\bar{R}|^2) d\eta. \end{aligned}$$

The second integral, which equals

$$\mathrm{Re}\, c \int |P|^{-2}(2\bar{P}RS - c|R|^2) d\eta,$$

can be made positive definite in the w_s (by choosing R properly) if the same is true of

$$W = \mathrm{Re} \int SR/P\, d\eta.$$

To see this one employs the same reasoning as that used at the end of the proof of Lemma 5. The quantity c must be taken real and sufficiently small. Thus, by Lemmas 3 and 5, we are through if we can pick R in such a way that W is positive definite in the w_s for each $\xi \neq 0$. Now the coefficient of $g_s h_t$ in W is

$$c_{st} = \int \eta^{s+t-2}/P \, d\eta,$$

and by Lemma 6 the $(m-q)\times(m-q)$ matrix (c_{st}) is non-singular. If we set $g_{m-r} = g_{m-r+1} = \cdots = g_{m-q} = 0$, we can solve the system

$$\sum_{t=1}^{m-q} c_{st} h_t = |\xi|^{2s+1} \bar{g}_s$$

for the h_t. Since the $\bar{g}_s$ are linear in the $\bar{w}_s$, so are the h_t, and by uniqueness it is easily checked that h_t is homogeneous in ξ of degree $2m-t+1$. Moreover, for this choice of R,

$$W = \sum_{s=1}^{m-r} |\xi|^{2s+1} |g_s|^2.$$

and hence cannot vanish unless all the g_s do. But by the ellipticity of A, this cannot happen without all the w_s vanishing (Lemma 4). Hence W is a positive definite quadratic form in the w_s. This completes the proof.

Necessity. That A must be elliptic follows from Lemma 7. We now prove that

(IV) $\quad |u|_m{}^2 \leqq K(\|Au\|^2 + \|u\|^2)$ for all $u \in C^{*r}(G^*)$

cannot hold if $q > r$. (This is slightly stronger than the statement in the theorem and will be used in the next section.) We employ an extension of an example due to Aronszajn [1]. Assume for definiteness that $q = p_1 > r$. This means that, for any $\xi \neq 0$, there are complex numbers $z_1, z_2, \cdots, z_q$ such that $\operatorname{Im} z_s > 0$ and $P(\xi, z_s) = 0$ for $1 \leqq s \leqq q$. We may assume that G^* is so situated that $B^*{}_1$ contains the origin (see Section 3). Let ϕ be a function in $C^{*0}(G^*)$ which is identically 1 near the origin and such that $\partial\phi/\partial y = 0$ on $y = 0$. We first assume that all the z_s are different. Then we can find a set of q numbers b_s, not all zero, such that

$$\sum_{s=1}^{q} b_s z_s{}^t = 0. \qquad \text{for } 0 \leqq t < q-1.$$

Set $v(x,y) = \sum_{s=1}^{q} b_s(\xi x + z_s y + \epsilon i)^{\frac{1}{2}}$ and $u = \phi v$. Then $u \in C^{*r}(G^*)$, since

$$\partial^t u/\partial y^t \propto \phi \sum b_s z_s{}^t (\xi x + z_s y + \epsilon i)^{\frac{1}{2}-t}$$

which vanish on $y=0$ for $0 \leqq t < q-1$. The quantities $\| u \|$ and $\| Au \|$ remain bounded as $\epsilon \rightarrow 0$, the latter since

$$Av \propto \sum b_s P(\xi, z_s)(\xi x + z_s y + \epsilon i)^{\frac{1}{2}-m} \equiv 0.$$

At least one of the numbers b_s, say b_1, does not vanish. Let $Q(\xi, \eta)$ be a homogeneous polynomial having all the (ξ, z_s) but (ξ, z_1) as roots and let N be its corresponding operator. Then

$$Nv \propto b_1 Q(\xi, z_1)(\xi x + z_1 y + \epsilon i)^{\frac{1}{2}-m} \not\equiv 0.$$

Hence $\| Nu \| \rightarrow \infty$ as $\epsilon \rightarrow 0$ and (IV) cannot hold.

If not all the roots z_s are different, we set $v = \sum Y_s(\xi x + z_s y + \epsilon i)^{\frac{1}{2}}$, where Y_s is a polynomial in y of degree one less than the multiplicity of z_s. One then has enough arbitrary constants to insure that $u \in C^{*r}(G^*)$. The reader is spared the details.

Proof of Corollary 2. Following the proof of Theorem 4, we take $R = \bar{\gamma} \bar{S}$. Then $W = \int | P |^{-2} | S |^2 \operatorname{Re} \gamma P \, d\eta$, and hence $W > 0$ unless $S \equiv 0$. This can happen only if each $g_s = 0$ which in turn implies that each $w_s = 0$ (Lemma 4). The result again follows from Lemma 5.

It now remain only to prove Theorem 2 from Theorem 4. This will be done in the next section.

6. Proof of Theorem 2. We shall show that Theorems 1 and 2 hold for domains G of class C^m. The proof is essentially contained in Lemmas 8-12 which follow. In them we employ inequality (6) due to Ehrling [3] and Nirenberg [6], to which the reader is referred for proof.

Definition. A domain G is said to be in class C^s if every boundary point x of G has a neighborhood $\mathfrak{a}$ such that the closure of $\mathfrak{a} \cap G$ can be mapped in a one-to-one way onto the closure of a domain G^* of Section 3 with $\mathfrak{a} \cap B$ (the boundary of G) mapped into $x_n = 0$ and such that the map and its inverse are s times continuously differentiable.

LEMMA. *If* $G \in C^2$ *and* $s < t$, *then for every* $\epsilon > 0$ *sufficiently small there exists a constant* K *such that*

$$\| u \|_s^2 \leqq \epsilon \| u \|_t^2 + K \| u \|^2 \text{ for all } u \in C^0(G). \tag{6}$$

Let x be a point in n-space, and assume that A is a linear m-th order partial differential operator with coefficients continuous at x. Denote its characteristic polynomial by P, and let A' be the homogeneous m-th order operator with constant coefficients which equals the principal part of A at x. We now have

LEMMA 8. *There is a neighborhood* $\mathfrak{A}$ *of* x *such that*

$$\text{(III)} \qquad \| u \|_m^2 \leqq K(\| Au \|^2 + \| u \|^2) \text{ for all } u \in U(\mathfrak{A})^{6}$$

if and only if there is a neighborhood $\mathfrak{B}$ *of* x *such that*

$$\text{(III')} \qquad \| u \|_m^2 \leqq K(\| A'u \|^2 + \| u \|^2) \text{ for all } u \in U(\mathfrak{B}).$$

Proof. Suppose (III) holds. Since $Au = A'u + (A - A')u$, we have $\| Au \|^2 \leqq 2 \| A'u \|^2 + 2 \| (A - A')u \|^2$. In a small enough neighborhood of x, $\| (A - A')u \|^2 \leqq \epsilon \| u \|_m^2 + K \| u \|_{m-1}^2$, and hence, by (6), for any $\epsilon' > 0$, there is a K such that

$$\| Au \|^2 \leqq 2 \| A'u \|^2 + \epsilon' \| u \|_m^2 + K \| u \|^2$$

in a sufficiently small neighborhood of x. Combining this with (III) shows that we can find a neighborhood $\mathfrak{B}$ so small that

$$\| u \|_m^2 \leqq K(\| A'u \|^2 + \| u \|^2) + \tfrac{1}{2} \| u \|_m^2$$

for all $u \in U(\mathfrak{B})$. Thus (III') holds. The converse is proved in the same way.

In light of Lemma 7 we have

LEMMA 9. *There exists a neighborhood* $\mathfrak{A}$ *of* x *in which* (III) *holds if and only if* A *is elliptic at* x.

We now suppose that x is on the "flat part" of a domain G^* of Section 3 (i. e. on B^*_1).

LEMMA 10. *There is a neighborhood* $\mathfrak{A}$ *of* x *such that*

$$\text{(V)} \qquad \| u \|_m^2 \leqq K(\| Au \|^2 + \| u \|^2) \text{ for all } u \in C^{*r}(\mathfrak{A} \cap G^*)$$

if and only if there is a neighborhood $\mathfrak{B}$ *of* x *such that*

$$\| u \|_m^2 \leqq K(\| A'u \|^2 + \| u \|^2) \text{ for all } u \in C^{*r}(\mathfrak{B} \cap G^*).$$

Proof. Same as that for Lemma 8.

---

[6] See the beginning of Section 5 for the definition of $U(G)$.

If q is defined for A' as in Section 3, we see from Theorem 4 and its necessity proof that

LEMMA 11. *There exists a neighborhood* $\mathfrak{A}$ *of* x *in which* (V) *holds if and only if* A *is elliptic at* x *and* $q \leqq r$.

We now return to a general domain $G \in C^m$ and to an m-th order operator A with coefficients continuous in $\bar{G}$.

LEMMA 12 (Aronszajn). *A necessary and sufficient condition that* (I) *hold is that each point* x *of* $\bar{G}$ *has a neighborhood* $\mathfrak{A}$ *such that*

$$(7) \qquad \| u \|_m^2 \leqq K(\| Au \|^2 + \| u \|^2) \quad \textit{for all } u \in [C^r(G) \cap U(\mathfrak{A})].$$

Proof. The necessity is obvious. To show sufficiency, suppose that the condition is satisfied. Thus for each point x of $\bar{G}$, there is a neighborhood $\mathfrak{A}$ in which (7) holds. These neighborhoods cover $\bar{G}$, and, by the Heine-Borel theorem, there is a finite subset $(\mathfrak{A}_k)$ which does likewise. Let $1 \equiv \sum \zeta_k$ be a partition of unity subordinate to this covering. We may assume that the ζ_k are infinitely differentiable. Thus $u\zeta_k \in [C^r(G) \cap U(\mathfrak{A}_k)]$, and hence, by (7), $\| \zeta_k u \|_m^2 \leqq K(\| A\zeta_k u \|^2 + \| u \|^2)$ for all $u \in C^r(G)$. Summing over k, we obtain

$$(8) \qquad \sum \| \zeta_k u \|_m^2 \leqq K(\sum \| A\zeta_k u^2 \| + \| u \|^2).$$

Now

$$(9) \qquad \| u \|_m^2 = \| \sum \zeta_k u \|_m^2 \leqq K \sum \| \zeta_k u \|_m^2,$$

and since $A\zeta_k u = \zeta_k Au +$ terms of derivatives of u of order $< m$, we have, by (6),

$$(10) \quad \| A\zeta_k u \|^2 \leqq 2 \| \zeta_k Au \|^2 + K \| u \|_{m-1}^2 \leqq 2 \| Au \|^2 + \epsilon \| u \|_m^2 + K \| u \|^2.$$

Inequalities (8), (9) and (10) imply (I). Q.e.d.

We are now ready for the

Proof of Theorem 2. From Lemma 9, we see that ellipticity is essential in the interior of G. Now let x be a point of B, the boundary of G. By hypothesis, there is a neighborhood $\mathfrak{A}$ of x such that the closure of $\mathfrak{A} \cap G$ can be mapped in a certain way onto the closure of a domain G^* of Section 3. We can make this mapping in two steps. First rotate the coordinate axes until x_n is perpendicular to B at x, and then make the required transformation by changing only x_n but not the other x_k. (This can always be done).

What happens to A? It is transformed into a similar operator A_1 *and the quantity* q *defined for* A *in Section* 2 *equals the quantity* q *for* A_1 *in Lemma* 11. This in turn is the same for the operator $A_2 = J^{\frac{1}{2}} A_1$, where J is the Jacobian of the transformation. (These facts follow from the ellipticity of A.) We now merely note that (7) holds in $\mathfrak{A}$ if and only if

$$\| u \|_m^2 \leqq K(\| A_2 u \|^2 + \| u \|^2) \quad \text{for all} \quad u \in C^{*r}(G^*).$$

The result now follows from Lemmas 11 and 12.

Corollary 1 follows from Corollary 2 in the same way.

NEW YORK UNIVERSITY.

REFERENCES.

[1] N. Aronszajn, "On coercive integro-differential quadratic forms," *Conference on Partial Differential Equations*, University of Kansas, Summer 1954, pp. 94-106.

[2] F. E. Browder, "Regularity properties at the boundary of solutions of elliptic boundary value problems (abstract)," *Bulletin of the American Mathematical Society*, vol. 62 (1956), p. 381.

[3] G. Ehrling, "On a type of eigenvalue problems for certain elliptic differential operators," *Mathematica Scandinavica*, vol. 2 (1954), pp. 267-285.

[4] L. Gårding, "Dirichlet's problem for linear elliptic partial differential equations," *ibid.*, vol. 1 (1953), pp. 55-72.

[5] L. Hörmander, "On the theory of general partial differential operators," *Acta Mathematica*, vol. 94 (1955), pp. 161-284.

[6] L. Nirenberg, "Remarks on strongly elliptic partial differential equations," *Communications on Pure and Applied Mathematics*, vol. 8 (1955), pp. 649-675.

[7] O. V. Guseva, "On boundary problems for strongly elliptic systems," *Doklady Akademiia Nauk SSSR, N. S.*, vol. 102 (1955), pp. 1069-1072 (in Russian).

A NOTE ON CONSERVATIVE TRANSFORMATIONS AND THE RECURRENCE THEOREM.*[1]

By Louis Sucheston.

Let X be a space and $\mathcal{B}$ a σ-field of "measurable" subsets of X, that is a class of sets closed under countable set-operations, with $X \in \mathcal{B}$. Let $\mathcal{S}$ be a class of sets of $\mathcal{B}$; we may call elements of $\mathcal{S}$ "sets of measure 0." Assume that a multi-valued transformation T is defined on X, i. e., a function which lets correspond to each point $x \in X$ a non-empty set $Tx \subset X$. The empty set is denoted Θ. $T^{-1}A$ is the set of points x such that $Tx \cap A \neq \Theta$. The transformation T will be always assumed measurable, that is such that $T^{-1}\mathcal{B} \subset \mathcal{B}$. We shall say that T is *conservative* if $A \in \mathcal{S}$ whenever a set $A \in \mathcal{B}$ is disjoint with all sets $T^{-i}A$, $i = 1, 2, \cdots$. It has been proved by Halmos ([1], pp. 736-738, see also [2], p. 13), that any power T^n of a conservative transformation T is again conservative. Halmos assumes that T is single-valued, so that Tx is a single point for each x, that T is one-to-one and that T^{-1} is measurable. The proof, based on an argument of E. Hopf ([3], p. 391), is rather difficult. We propose here a simple proof of this result, which does not make use of the above assumptions. A version of the recurrence theorem extended in the same sense is then derived (compare [1], p. 747), with a corollary about a subsequence of the sequence $T^{-n}A$.

Theorem A. *If $\mathcal{S}$ is closed under finite set-unions and if a transformation T is conservative, then T^n for $n = 1, 2, \cdots$ is conservative.*

Proof. Let $A \in \mathcal{B}$ and

$$(1) \qquad A \cap T^{-in}A = \Theta \qquad i = 1, 2, \cdots.$$

We have to show that $A \in \mathcal{S}$. We arrange all sets $T^{-k}A$, $k = 0, 1, \cdots$ in the following scheme:

---

* Received October 26, 1956.

[1] This work was in part supported by the National Science Foundation Grant NSF-G1975. The author gratefully acknowledges his indebtedness to Professor G. Lorentz for his encouragement.

$$\begin{array}{lll}
A, & T^{-1}A, \cdots, & T^{-(n-1)}A \\
T^{-n}A, & T^{(n+1)}A, \cdots, & T^{-(2n-1)}A \\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\
T^{-in}A, & T^{-(in+1)}A, \cdots, & T^{-(in+n-1)}A \\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot
\end{array}$$

Let D_j, $j = 1, 2, \cdots, n$, be the set of points $x \in A$ which belong to exactly j columns of the scheme (2). We shall prove that

$$D_j \cap T^{-v} D_j = \Theta \qquad v = 1, 2, \cdots \tag{3}$$

and hence $A = \bigcup_{j=1}^{n} D_j \in \mathcal{S}$. If (3) is not true for some $v \geqq 1$, there exists a point $x \in D_j \cap T^{-v} D_j$. There is a point y such that $y \in T^v x$, $y \in D_j$ and this last relation implies that

$$y \in T^{-n_1}A, \qquad y \in T^{-n_2}A, \cdots, \qquad y \in T^{-n_j}A \tag{4}$$

where $n_1, \cdots, n_j$ is some set of non-negative integers, different modulo n. Since $x \in T^{-v} y$, we have

$$x \in T^{-(n_1+v)}A, \qquad x \in T^{-(n_2+v)}A, \cdots, \qquad x \in T^{-(n_j+v)}A \tag{5}$$

where $n_1 + v, \cdots, n_j + v$ are *positive* integers, different modulo n. However, we know that $x \in D_j \subset A = T^0 A$ and by (1) that $x \notin T^{-ni}A$, $i = 1, 2, \cdots$. Therefore none of the numbers $n_s + v$, $s = 1, 2, \cdots, j$ is congruent to 0 modulo n. It follows that x belongs to the sets $T^0 A, T^{-(n_1+v)}A, \cdots, T^{-(n_j+v)}A$ which are in $j + 1$ different columns. This contradicts $x \in D_j$ and proves the theorem.

We deduce now the recurrence theorem. A point $x \in A$ is called *recurrent* under T (with respect to A) if there exists an infinite set of positive integers n_i such that $T^{n_i} x \cap A \neq \Theta$ for $i = 1, 2, \cdots$.

THEOREM B. (*Recurrence Theorem*). *Assume that $\mathcal{S}$ is closed under countable set-unions, let A be a set of $\mathfrak{B}$ and E the set of points of A not recurrent under a conservative transformation T. Then $E \in \mathcal{S}$.*

Proof. Put $E_n = \bigcap_{j=0}^{\infty} (A - T^{-(n+j)}A)$. Then for any $v \geqq n > 0$,

$$E_n \subset A - T^{-v}A \text{ and } T^{-v}E_n \subset T^{-v}A,$$

hence $E_n \cap T^{-iv}E_n = \Theta$ for $i = 1, 2, \cdots$ and by Theorem A, $E_n \in \mathcal{S}$. Therefore $E = \bigcup_{n=1}^{\infty} E_n \in \mathcal{S}$.

It follows also that "almost all" points of A are recurrent under *each* positive power T^n of T. It should be noted that there is a simple proof of the recurrence theorem (but not of the last remark), which does not depend on Theorem A (in [5], where some of Oxtoby's assumptions are not necessary).

We derive still a corollary under the assumption that $\mathcal{S}$ is an *σ-ideal* in $\mathcal{B}$, i.e., $\mathcal{S}$ is closed under finite set-unions and $E \cap A \in \mathcal{S}$ whenever $E \in \mathcal{S}$ and $A \in \mathcal{B}$. Let $A \in \mathcal{B}$, it follows from the proof of Theorem B that the set $E_1 = A - \bigcup_{i=1}^{\infty} (A \cap T^{-i}A)$ belongs to $\mathcal{S}$. Hence, if $A \in \mathcal{B} - \mathcal{S}$, there is an integer $r > 0$ such that $A \cap T^{-r}A \in \mathcal{B} - \mathcal{S}$. Put $B = A \cap T^{-r}A$ and consider B and T^{r+1} instead of A and T. There is an integer $s > r$ such that $B \cap T^{-s}B \in \mathcal{B} - \mathcal{S}$, hence $C = A \cap T^{-r}A \cap T^{-s}A \in \mathcal{B} - \mathcal{S}$, for $T^{-s}B \subset T^{-s}A$. Consider now C and T^{s+1}, etc. The argument can be carried on indefinitely. If $A_1, \cdots, A_k \in \mathcal{B}$ and $\bigcap_{i=1}^{k} A_i \in \mathcal{B} - \mathcal{S}$, the collection of sets $A_1, \cdots, A_k$ will be called *compatible.* (The word has its intuitive sense if a probability measure is defined on $\mathcal{B}$ vanishing on $\mathcal{S}$. See then [4] and [6] for additional information.) We have proved the following:

COROLLARY. *Assume that $\mathcal{S}$ is an σ-ideal in $\mathcal{B}$, let A be a set, T a conservative transformation and $A_n = T^{-n}A$ for $n = 1, 2, \cdots$. Then for any set $A_k \in \mathcal{B} - \mathcal{S}$ of the sequence $\{A_n\}$, there exists an infinite subsequence $\{A_{n_i}\}$ beginning with A_k and such that any finite collection of sets A_{n_i} is compatible.*

We add the following remarks: Our definition of a conservative transformation T is different from Halmos' definition ([2], p. 12) which requires that $A \in \mathcal{S}$ whenever $A \in \mathcal{B}$ and the sets $T^{-i}A$, $i = 0, 1, \cdots$ are pairwise disjoint. Halmos considers also incompressible transformations: T is incompressible if $T^{-1}A - A \in \mathcal{S}$ whenever $A \in \mathcal{B}$ and $A \subset T^{-1}A$ ([2], p. 13). We assume (to simplify) that $\mathcal{S}$ is an σ-ideal in $\mathcal{B}$. The relation between the different considered notions is the following: If a transformation is incompressible, it is conservative in our sense; if a transformation is conservative in our sense, it is conservative in the sense of Halmos. It can be shown by simple examples (and such that a probability measure can be defined on $\mathcal{B}$, vanishing on $\mathcal{S}$), that the inverse implications do not hold, and also that with Halmos' definition the recurrence theorem does not hold for multivalued transformations. This is of course the reason for which this definition has been here modified. For single-valued transformations (only this case is considered by Halmos and Oxtoby) all three notions coincide.

WAYNE STATE UNIVERSITY.

REFERENCES.

[1] P. Halmos, "Invariant measures," *Annals of Mathematics*, vol. 48 (1947), pp. 735-754.

[2] ———, *Ergodic Theory*, University of Chicago (1955), mimeographed.

[3] E. Hopf, "Theory of measure and invariant integrals," *Transactions of the American Mathematical Society*, vol. 34 (1932), pp. 373-393.

[4] A. Khintchine, "Eine Verschärfung des Poincaré'schen Wiederkehrsatzes," *Compositio Mathematica*, vol. 1 (1935), pp. 177-179.

[5] J. C. Oxtoby, *Category and measure*, lectures at the Summer Meeting of the Mathematical Association of America, Seattle, 1956 (unpublished).

[6] C. Visser, "On Poincaré's recurrence theorem," *Bulletin of the American Mathematical Society*, vol. 42 (1936), pp. 397-400.

ERRATA.

M. Kuranishi, "On E. Cartan's prolongation theorem of exterior differential systems," this JOURNAL, vol. 79 (1957), pp. 1-47.

P. 20, lines 12 and 23: Instead of "Since $d(d(f \circ \rho_{l-1}{}^{l})) = 0$,

$$(22) \qquad D_k \circ D_h = D_h \circ D_k, \qquad (h, k = 1, \cdots, p).",$$

read "Since $d(d(f \circ \rho_{l-1}{}^{l})) = 0$, for any $h, k = 1, \cdots, p$,

$$(22) \qquad D_k \circ D_h f - D_h \circ D_k f \equiv 0 \quad (\operatorname{mod} \Theta_{\phi\,;ij\,;}\,; \phi \in \Sigma^{[2]}, \quad i, j = 1, \cdots, p)";$$

this should be inserted in the next line of the formula (25).

P. 20, line 6 from the bottom: The formula (26) should be replaced by

$$\text{"}(26) \qquad \Theta_{\phi\,;ij\,;\,k_1 \cdots k_{l-1}} = \sum (l-1)!^{-1} D_{h_{l-1}} \circ \cdots \circ D_{h_1}(\Theta_{\phi\,;ij\,;}),$$

where the summation is with respect to all $(h_1, \cdots, h_{l-1})$ which is a permutation of $(k_1, \cdots, k_{l-1})$."

P. 21, line 3: Instead of "$B_{\phi\,;ij\,;\,\mathcal{K}_{l-1}}$ are defined inductively by the formula:", read "By (22), it follows that"

P. 21, line 4: Instead of "$B_{\phi\,;ij\,;\,k_1 \cdots k_{l-1}} = \ldots$", read

$$\text{"}B_{\phi\,;ij\,;\,k_1 \cdots k_{l-1}} \equiv \ldots\text{"}.$$

P. 21, line 6: Insert

$$\text{"}(\operatorname{mod} \Theta^{\psi}{}_{;fg\,;\,h_1 \cdots h_{l-3}}\,; \psi \in \Sigma^{[2]}, f, g, \cdots, h_1, \cdots, h_{l-3} = 1, \cdots, p)\text{"}$$

at the beginning of the line.

P. 21, line 13: Instead of "$(\operatorname{mod} \pi_l)$", read "$(\operatorname{mod}(\Pi_l), \mathcal{R}_{l-2}{}^{[0]}\Sigma)$".

P. 21, line 14: Insert "$(\operatorname{mod}\,(\Pi_l), \mathcal{R}_{l-2}{}^{[0]}\Sigma)$".

P. 22, lines 15 and 17: Twice instead of

$$\text{"}\operatorname{mod}(v^{\lambda}{}_{;k}, v^{\lambda}{}_{j_1\,;k}, \cdots, v^{\lambda}{}_{j_1 \cdots j_{l-1}\,;\,k})\text{"},$$

read "$(\operatorname{mod} v^{\lambda}{}_{;k}, v^{\lambda}{}_{j_1\,;k}, \cdots, v^{\lambda}{}_{j_1 \cdots j_{l-1}\,;\,k}, v_k{}^{\alpha}, \mathcal{R}_{l-1}{}^{[0]}\Sigma)$".

CALCUTTA * UNIVERSITY * CENTRAL LIBRARY

ON c.s.s. COMPLEXES.*

By Daniel M. Kan.

---

1. **Introduction.** It was indicated in [3] how the usual notions of homotopy theory may be defined for cubical complexes which satisfy a certain extension condition. In the same manner (see [9]) these notions may be defined for complete semi-simplicial (c. s. s.) complexes which satisfy the following c. s. s. version of the extension condition. The notation used will be that of [2] except that the face and degeneracy operators will be denoted by ϵ^i and η^j (instead of ϵ_n^i and η_n^j).

Definition (1.1). A c. s. s. complex K is said to satisfy the *extension condition* if for every pair of integers (k, n) with $0 \leqq k \leqq n$ and for every n $(n-1)$-simplices $\sigma_0, \cdots, \sigma_{k-1}, \sigma_{k+1}, \cdots, \sigma_n \in K$ such that $\sigma_i\epsilon^{j-1} = \sigma_j\epsilon^i$ for $i < j$ and $i \neq k \neq j$, there exists an *n-simplex* $\sigma \in K$ such that $\sigma\epsilon^i = \sigma_i$ for $i = 0, \cdots, \hat{k}, \cdots, n$.

Let $\mathcal{S}$ be the category of c. s. s. complexes and c. s. s. maps and let $\mathcal{S}_E$ be its full subcategory generated by the c. s. s. complexes which satisfy the extension condition.

Many interesting c. s. s. complexes do not satisfy the extension condition; for example the finite c. s. s. complexes (finite = with only a finite number of non-degenerate simplices). The definitions of some homotopy notions, such as the homology groups, apply to all c. s. s. complexes, but the definition of the homotopy groups of [9], for instance, cannot be carried over to c. s. s. complexes which are not in $\mathcal{S}_E$.

In order to extend the definitions of all homotopy notions defined on the category $\mathcal{S}_E$ to the whole category $\mathcal{S}$ one needs what will be called an H-pair, i. e., a pair (Q, q) consisting of

(i) a functor $Q\colon \mathcal{S} \to \mathcal{S}_E$,

(ii) a natural transformation $q\colon E \to Q$ (where $E\colon \mathcal{S} \to \mathcal{S}$ denotes the identity functor), satisfying the following conditions:

(a) The functor Q maps homotopic maps into homotopic maps.

(b) Let $K \in \mathcal{S}_E$, then the map $qK\colon K \to QK$ is a homotopy equivalence.

---

* Received September 20, 1956.

(c) Let $K \in \mathcal{S}$ and let $f\colon QK \to QK$ be a map such that commutativity holds in the diagram

$$\begin{tikzcd} & QK \arrow[dd, "f"] \\ K \arrow[ur, "qK"] \arrow[dr, "qK"'] & \\ & QK \end{tikzcd}$$

Then f is a homotopy equivalence.

In view of condition (a) every homotopy notion on the category $\mathcal{S}_E$ yields by composition with the functor Q a homotopy notion on the whole category $\mathcal{S}$. Condition (b) implies that on the category $\mathcal{S}_E$ the homotopy notions induced by the functor Q coincide with the original ones. Condition (c) essentially ensures the uniqueness of the homotopy notions induced by Q; if (R, r) is another H-pair, then Q and R induce the same homotopy notions. In particular QK and RK have the same homotopy type, even if K does not satisfy the extension condition.

An example of an H-pair is the following. Let $S|\ |\colon \mathcal{S} \to \mathcal{S}_E$ be the functor which assigns to a c. s. s. complex K the simplicial singular complex $S|K|$ of the geometrical realization $|K|$ of K and let $j\colon E \to |\ |$ be the natural transformation which assigns to a c. s. s. complex K the natural embedding $jK\colon K \to S|K|$. Then it is readily seen that the pair $(S|\ |, j)$ is an H-pair.

Although the existence of an H-pair is sufficient in order to do homotopy theory on the whole category $\mathcal{S}$, it is sometimes convenient to have an H-pair which (unlike the pair $(S|\ |, j)$) may be defined in terms of c. s. s. complexes and c. s. s. maps only. Such an H-pair $(\mathrm{Ex}^\infty, \mathrm{e}^\infty)$ will be defined in this paper. A useful property of the functor $\mathrm{Ex}^\infty\colon \mathcal{S} \to \mathcal{S}_E$ is that it preserves fibre maps.

The main tool used in the definition of the functor Ex^∞ is what we call the *extension* $\mathrm{Ex}\,K$ of a c. s. s. complex K, which is in a certain sense dual to the *subdivision* $\mathrm{Sd}\,K$ of K. More precisely: let K and L be c. s. s. complexes, then there exists (in a natural way) a one-to-one correspondence between the c. s. s. maps $\mathrm{Sd}\,K \to L$ and the c. s. s. maps $K \to \mathrm{Ex}\,L$. In the terminology of [6] this means that the functor Ex is a right adjoint of the functor Sd.

The simplicial approximation theorem may be generalized to c. s. s. complexes roughly as follows: let $K, L \in \mathcal{S}$, K finite, then every continuous map $f\colon |K| \to |L|$ is homotopic with the geometrical realization of a c. s. s.

map $g\colon \mathrm{Sd}^n K \to L$ for some n. Using the adjointness of the functors Sd and Ex a dual theorem may be obtained which involves a c. s. s. map $h\colon K \to \mathrm{Ex}^n L$ instead of $g\colon \mathrm{Sd}^n K \to L$. This dual theorem may be strengthened as follows: let $K \in \mathcal{S}$ and $L \in \mathcal{S}_E$, then every continuous map $f\colon |K| \to |L|$ is homotopic with the geometrical realization of a c. s. s. map $h\colon K \to L$. It is essentially because of this property that, as far as homotopy theory is concerned, the c. s. s. complexes which satisfy the extension condition "*behave like topological spaces.*"

The paper is divided into two chapters. In Chapter I the definitions and results are stated; most of the proofs are given in Chapter II.

The results of this paper were announced in [5].

Chapter I. Definitions and results.

2. The standard simplices and their subdivision. For each integer $n \geqq 0$ let $[n]$ denote the *ordered set* $(0, \cdots, n)$. By a map $\alpha\colon [m] \to [n]$ we mean a *monotone function*, i. e., a function such that $\alpha(i) \leqq \alpha(j)$ for $0 \leqq i \leqq j \leqq m$.

For each integer $n \geqq 0$ the *standard n-simplex* $\Delta[n]$ is the c. s. s. complex defined as follows. A q-simplex of $\Delta[n]$ is a map $\sigma\colon [q] \to [n]$. For each map $\beta\colon [p] \to [q]$ the p-simplex $\sigma\beta$ is defined as the composite map

$$[p] \xrightarrow{\beta} [q] \xrightarrow{\sigma} [n].$$

For each map $\alpha\colon [m] \to [n]$ let $\Delta\alpha\colon \Delta[m] \to \Delta[n]$ be the c. s. s. map which assigns to a q-simplex $\tau \in \Delta[m]$ the composite map

$$[q] \xrightarrow{\tau} [m] \xrightarrow{\alpha} [n].$$

The *subdivision* of $\Delta\ [n]$ is the c. s. s. complex $\Delta'[n]$ defined as follows. A q-simplex of $\Delta'[n]$ is a sequence $(\sigma_0, \cdots, \sigma_q)$ where the σ_i are *non-degenerate* simplices of $\Delta[n]$ (i. e., the map $\sigma_i\colon [\dim \sigma_i] \to [n]$ is a monomorphism) and σ_i *lies on* σ_{i+1} (i. e.. $\sigma_i = \sigma_{i+1}\alpha$ for some α) for all i. For each map $\beta\colon [p] \to [q]$ we have $(\sigma_0, \cdots, \sigma_q)\beta = (\sigma_{\beta(0)}, \cdots, \sigma_{\beta(p)})$.

The *subdivision* of $\Delta\alpha$ is the c. s. s. map $\Delta'\alpha\colon \Delta'[m] \to \Delta'[n]$ given by $\Delta'\alpha(\tau_0, \cdots, \tau_q) = (\sigma_0, \cdots, \sigma_q)$, where σ_i is the unique non-degenerate simplex of $\Delta[n]$ for which (see [2]) there exist an epimorphism $\gamma_i\colon [\dim \tau_i] \to [\dim \sigma_i]$ such that commutativity holds in the diagram

$$\begin{tikzcd}[\dim \tau_i] \arrow[r, "\tau_i"] \arrow[d, "\gamma_i"] & [m] \arrow[d, "\alpha"] \\ [\dim \sigma_i] \arrow[r, "\sigma_i"] & [n]\end{tikzcd} \tag{2.1}$$

For each integer $n \geqq 0$ let $\delta[n] : \Delta'[n] \to \Delta[n]$ be the c. s. s. map which assigns to a q-simplex $(\sigma_0, \cdots, \sigma_q) \in \Delta'[n]$ the q-simplex $\sigma \in \Delta[n]$, i. e., the map $\sigma : [q] \to [n]$, given by $\sigma(i) = \sigma_i(\dim \sigma_i)$, $0 \leqq i \leqq q$.

LEMMA (2.2). *For each map $\alpha : [m] \to [n]$ commutativity holds in the diagram*

$$\begin{tikzcd}\Delta[m] \arrow[r, "\Delta\alpha"] & \Delta[n] \\ \Delta'[m] \arrow[r, "\Delta'\alpha"] \arrow[u, "\delta{[m]}"] & \Delta'[n] \arrow[u, "\delta{[n]}"']\end{tikzcd} \tag{2.2a}$$

Proof. It follows from the definitions that for every q-simplex $(\tau_0, \cdots, \tau_q) \in \Delta'[m]$ and each integer i with $0 \leqq i \leqq q$,

$$(\Delta\alpha \circ \delta[m])(\tau_0, \cdots, \tau_q)(i) = \alpha\tau_i(\dim \tau_i),$$

$$(\delta[n] \circ \Delta'\alpha)(\tau_0, \cdots, \tau_q)(i) = \delta[n](\sigma_0, \cdots, \sigma_q)(i) = \sigma_i(\dim \sigma_i),$$

where σ_i is the unique non-degenerate simplex of $\Delta[n]$ for which there exists an epimorphism γ_i such that commutativity holds in diagram (2.1). Because γ_i is onto,

$$\alpha\tau_i(\dim \tau_i) = \sigma_i\gamma_i(\dim \tau_i) = \sigma_i(\dim \sigma_i).$$

Hence commutativity holds in diagram (2.2a).

3. The extension of a c. s. s. complex. The *extension* of a c. s. s. complex K is the c. s. s. complex $\operatorname{Ex} K$ defined as follows. An n-simplex of $\operatorname{Ex} K$ is a c. s. s. map $\sigma : \Delta'[n] \to K$. For each map $\alpha : [m] \to [n]$ the m-simplex $\sigma\alpha$ is the composite map

$$\Delta'[m] \xrightarrow{\Delta'\alpha} \Delta'[n] \xrightarrow{\sigma} K.$$

Similarly the *extension* of a c. s. s. map $f : K \to L$ is the c. s. s. map $\operatorname{Ex} f : \operatorname{Ex} K \to \operatorname{Ex} L$ which assigns to every n-simplex $\sigma \in \operatorname{Ex} K$ the composite map

$$\Delta'[n] \xrightarrow{\sigma} K \xrightarrow{f} L.$$

Clearly the function Ex so defined is a covariant functor $\mathrm{Ex}\colon \mathcal{S} \to \mathcal{S}$. By Ex^n we shall mean the functor Ex applied n times.

For c. s. s. complex K define a monomorphism $eK\colon K \to \mathrm{Ex}\, K$ as follows. For every n-simplex $\sigma \in K$, $(eK)\sigma$ is the composite map

$$\Delta'[n] \xrightarrow{\delta[n]} \Delta[n] \xrightarrow{\phi\sigma} K,$$

where $\phi_\sigma\colon \Delta[n] \to K$ is the unique map such that $\phi_\sigma \alpha = \sigma\alpha$ for all $\alpha \in \Delta[n]$. It follows from Lemma (2.2) that the function e is a natural transformation $e\colon E \to \mathrm{Ex}$ (where $E\colon \mathcal{S} \to \mathcal{S}$ denotes the identity functor), i. e., for every c. s. s. map $f\colon K \to L$ commutativity holds in the diagram

$$\begin{tikzcd}
K \arrow[r, "f"] \arrow[d, "eK"] & L \arrow[d, "eL"] \\
\mathrm{Ex}\, K \arrow[r, "\mathrm{Ex}\, f"] & \mathrm{Ex}\, L
\end{tikzcd}$$

We shall denote by $e^nK\colon K \to \mathrm{Ex}^n K$ the composite monomorphism

$$K \xrightarrow{eK} \mathrm{Ex}\, K \xrightarrow{e(\mathrm{Ex}\, K)} \cdots \xrightarrow{e(\mathrm{Ex}^{n-1} K)} \mathrm{Ex}^n K.$$

LEMMA (3.1). *The functor* $\mathrm{Ex}\colon \mathcal{S} \to \mathcal{S}$ *maps homotopic maps into homotopic maps.*

The proof will be given in Section 9.

An important property of the functor Ex is that if it is twice applied to a c. s. s. complex K, then the resulting complex $\mathrm{Ex}^2 K$ partially satisfies the extension condition; if $\rho_0, \cdots, \rho_{k-1}, \rho_{k+1}, \cdots, \rho_n \in \mathrm{Ex}^2 K$ are n $(n-1)$-simplices which "match" and which are in the image of $\mathrm{Ex}\, K$ under the map $e(\mathrm{Ex}\, K)\colon \mathrm{Ex}\, K \to \mathrm{Ex}^2 K$, then there exists an n-simplex $\rho \in \mathrm{Ex}^2 K$ (not necessarily in the image of $\mathrm{Ex}\, K$) such that $\rho\epsilon^i = \rho_i$ for $i \neq k$. An exact formulation is given in the following lemma.

LEMMA (3.2). *Let* $K \in \mathcal{S}$. *Then for every pair of integers* (k, n) *with* $0 \leqq k \leqq n$ *and for* n $(n-1)$*-simplices* $\tau_0, \cdots, \tau_{k-1}, \tau_{k+1}, \cdots, \tau_n \in \mathrm{Ex}\, K$ *such that* $\tau_i\epsilon^{j-1} = \tau_j\epsilon^i$ *for* $i < j$ *and* $i \neq k \neq j$, *there exists an n-simplex* $\rho \in \mathrm{Ex}^2 K$ *such that* $\rho\epsilon^i = (e(\mathrm{Ex}\, K))\tau_i$ *for* $i = 0, \cdots, \hat{k}, \cdots, n$.

The proof will be given in Section 10.

Another useful property of the functor Ex is that it preserves fibre maps. This is stated in Lemma (3.4).

Definition (3.3). A c.s.s. map $f\colon K \to L$ is called a *fibre map* if for each pair of integers (k, n) with $0 \leqq k \leqq n$, for every n $(n-1)$-simplices $\tau_0, \cdots, \tau_{k-1}, \tau_{k+1}, \cdots, \tau_n \in K$ such that $\tau_i\epsilon^{j-1} = \tau_j\epsilon^i$ for $i < j$ and $i \neq k \neq j$ and for every n-simplex $\rho \in L$ such that $\rho\epsilon^i = f\tau_i$ for $i = 0, \cdots, \hat{k}, \cdots, n$, there exists an n-simplex $\tau \in K$ such that $f\tau = \rho$ and $\tau\epsilon^i = \tau_i$ for $i = 0, \cdots, k, \cdots, n$. Let $\phi \in L$ be a 0-simplex. Then the counter image of ϕ and its degeneracies is called *the fibre of f over ϕ*. It is denoted by $F(f, \phi)$.

LEMMA (3.4). *Let $f\colon K \to L$ be a fibre map and let $\phi \in L$ be a 0-simplex. Then* $\mathrm{Ex}\, f\colon \mathrm{Ex}\, K \to \mathrm{Ex}\, L$ *is a fibre map and* $\mathrm{Ex}(F(f, \phi)) = F(\mathrm{Ex}\, f, (eL)\phi)$.

The proof will be given in Section 11.

Let $f\colon K \to \Delta[0]$ be a fibre map, then it follows readily from the fact that $\Delta[0]$ has only one simplex in every dimension that $K \in \mathcal{S}_E$. Conversely $K \in \mathcal{S}_E$ implies that the (unique) map $f\colon K \to \Delta[0]$ is a fibre map. As $\mathrm{Ex}\, \Delta[0] \approx \Delta[0]$ Lemma (3.4) thus implies

COROLLARY (3.5). *If $K \in \mathcal{S}_E$, then* $\mathrm{Ex}\, K \in \mathcal{S}_E$.

The following lemmas relate the homology groups of K and $\mathrm{Ex}\, K$ and, if $K \in \mathcal{S}_E$, their homotopy types.

LEMMA (3.6). *Let $K \in \mathcal{S}$. Then the map $eK\colon K \to$* $\mathrm{Ex}\, K$ *induces isomorphisms of the homology groups, i.e.,* $(eK)_*\colon H_*(K) \approx H_*(\mathrm{Ex}\, K)$.

The proof will be given in Section 12.

LEMMA (3.7). *Let $K \in \mathcal{S}_E$. Then the map $eK\colon K \to$* $\mathrm{Ex}\, K$ *is a homotopy equivalence.*

The proof will be given in Section 13.

4. The functor Ex$^\infty$.

Let K be a c.s.s. complex. Consider the sequence

$$\begin{tikzcd} K \arrow[r, "eK"] & \mathrm{Ex}\, K \arrow[r, "e(\mathrm{Ex}\, K)"] & \mathrm{Ex}^2 K \arrow[r, "e(\mathrm{Ex}^2 K)"] & \mathrm{Ex}^3 K \arrow[r] & \cdots \end{tikzcd}$$

and let $\mathrm{Ex}^\infty K$ be the direct limit of this sequence. The n-simplices of $\mathrm{Ex}^\infty K$ then are the pairs (σ, q) where $\sigma \in \mathrm{Ex}^q K$ is an n-simplex; two n-simplices (σ, q) and $(\tau, p+q)$ are considered equal if and only if $(e^p(\mathrm{Ex}^q K))\sigma = \tau$. For each map $\alpha\colon [m] \to [n]$, $(\sigma, q)\alpha = (\sigma\alpha, q)$. Similarly for a c.s.s. map $f\colon K \to L$ let $\mathrm{Ex}^\infty f\colon \mathrm{Ex}^\infty K \to \mathrm{Ex}^\infty L$ be the induced map given by $f(\sigma, q) = (f\sigma, q)$. Clearly the function Ex^∞ so defined is a covariant functor.

For a c. s. s. complex K denote by $e^{\infty} K\colon K \to \operatorname{Ex}^{\infty} K$ the limit monomorphism

$$K \xrightarrow{eK} \operatorname{Ex} K \xrightarrow{e(\operatorname{Ex} K)} \cdots \to \operatorname{Ex}^{\infty} K$$

i. e., $(e^{\infty} K)\sigma = ((eK)\sigma, 1)$ for every simplex $\sigma \in K$. Naturality of the function e^{∞} follows immediately from the naturality of e.

THEOREM (4.1). *The functor* $\operatorname{Ex}^{\infty}$ *maps homotopic maps into homotopic maps.*

The proof is similar to that of Lemma (3.1) (see Section 9), using $\operatorname{Ex}^{\infty}$ and e^{∞} instead of Ex and e.

An important property of the functor $\operatorname{Ex}^{\infty}$ is:

THEOREM (4.2). $\operatorname{Ex}^{\infty} K \in \mathcal{S}_E$ *for all objects* $K \in \mathcal{S}$, i. e., $\operatorname{Ex}^{\infty}$ *is a functor* $E^{\infty}\colon \mathcal{S} \to \mathcal{S}_E$.

This follows immediately from Lemma (3.2) and the definition of $\operatorname{Ex}^{\infty}$.

Another useful property of the functor $\operatorname{Ex}^{\infty}$ is that it preserves fibre maps.

THEOREM (4.3). *Let* $f\colon K \to L$ *be a fibre map and let* $\phi \in L$ *be a 0-simplex. Then* $\operatorname{Ex}^{\infty} f\colon \operatorname{Ex}^{\infty} K \to \operatorname{Ex}^{\infty} L$ *is a fibre map and* $\operatorname{Ex}^{\infty}(F(f, \phi)) = F(\operatorname{Ex}^{\infty} f, (e^{\infty} L)\phi)$.

This follows immediately from Lemma (3.4).

We shall now relate the homology groups of K and $\operatorname{Ex}^{\infty} K$ and, if $K \in S_E$, their homotopy types.

THEOREM (4.4). *Let* $K \in \mathcal{S}$. *Then the map* $e^{\infty} K\colon K \to \operatorname{Ex}^{\infty} K$ *induces isomorphisms of the homology groups, i. e.,* $(e^{\infty} K)_*\colon H_*(K) \approx H_*(\operatorname{Ex}^{\infty} K)$.

This follows immediately from Lemma (3.6).

Similarly, Lemma (3.7) implies.

THEOREM (4.5). *Let* $K \in \mathcal{S}_E$. *Then the map* $eK\colon K \to \operatorname{Ex}^{\infty} K$ *is a homotopy equivalence.*

Let K be a c. s. s. complex which does *not* satisfy the extension condition. Then the homotopy type of $\operatorname{Ex}^{\infty} K$ cannot be related to the homotopy type of K because the latter has (not yet) been defined. However the homotopy type of $\operatorname{Ex}^{\infty} K$ may be related to K as follows:

THEOREM (4.6). *Let* $K \in \mathcal{S}$ *and let* $f\colon \operatorname{Ex}^\infty K \to \operatorname{Ex}^\infty K$ *be a c.s.s. map such that commutativity holds in the diagram*

$$\begin{tikzcd} & \operatorname{Ex}^\infty K \arrow[d, "f"] \\ K \arrow[ur, "e^\infty K"] \arrow[r, "e^\infty K"'] & \operatorname{Ex}^\infty K \end{tikzcd}$$

Then f *is a homotopy equivalence.*

The proof will be given in Section 14.

5. Homotopy notions induced on $\mathcal{S}$.

Definition (5.1). A pair (Q, q) where $Q\colon \mathcal{S} \to \mathcal{S}_E$ is a covariant functor and $q\colon E \to Q$ a natural transformation (E denotes the identity functor $E\colon \mathcal{S} \to \mathcal{S}$), is called an *H-pair* if the following conditions are satisfied:

(a) The functor $Q\colon \mathcal{S} \to \mathcal{S}_E$ maps homotopic maps into homotopic maps

(b) Let $K \in \mathcal{S}_E$. Then the map $qK\colon K \to QK$ is a homotopy equivalence

(c) Let $K \in \mathcal{S}$ and let $f\colon QK \to QK$ be a c.s.s. map such that commutativity holds in the diagram

$$\begin{tikzcd} & QK \arrow[d, "f"] \\ K \arrow[ur, "qK"] \arrow[r, "qK"'] & QK \end{tikzcd}$$

Then f is a homotopy equivalence.

Example (5.2). The pair $(\operatorname{Ex}^\infty, e^\infty)$ is an H-pair; this follows directly from Theorems (4.1), (4.5) and (4.6).

A more exact formulation of the statements about H-pairs made in the introduction will be given in Theorems (5.4), (5.5) and (5.8).

Definition (5.3). By a *homotopy notion* on the category $\mathcal{S}$ (resp. $\mathcal{S}_E$) with values in a category $\mathfrak{Z}$ we mean a functor $N\colon \mathcal{S} \to \mathfrak{Z}$ (resp. $N\colon \mathcal{S}_E \to \mathfrak{Z}$) such that for two maps $f, g \in \mathcal{S}$ (resp. $\mathcal{S}_E$) $f \simeq g$ implies $Nf = Ng$.

THEOREM (5.4). *Let* $N\colon \mathcal{S}_E \to \mathcal{Z}$ *be a homotopy notion on* $\mathcal{S}_E$ *and let* (Q,q) *be an H-pair. Then the composite functor*

$$\mathcal{S} \xrightarrow{Q} \mathcal{S}_E \xrightarrow{N} \mathcal{Z}$$

is a homotopy notion on $\mathcal{S}$.

This is an immediate consequence of condition (5.1a).

Let $J\colon \mathcal{S}_E \to \mathcal{S}$ be the inclusion functor and let $N\colon \mathcal{S}_E \to \mathcal{Z}$ be a homotopy notion on $\mathcal{S}_E$. We then want to compare the composite functor

$$\mathcal{S}_E \xrightarrow{J} \mathcal{S} \xrightarrow{Q} \mathcal{S}_E \xrightarrow{N} \mathcal{Z}$$

i.e., the restriction to $\mathcal{S}_E$ of the homotopy notion on $\mathcal{S}$ induced by the functor Q, with the original homotopy notion N on $\mathcal{S}_E$. The following theorem then asserts that these functors differ only by a natural equivalence.

THEOREM (5.5). *Let* $N\colon \mathcal{S}_E \to \mathcal{Z}$ *be a homotopy notion on* $\mathcal{S}_E$ *and let* (Q,q) *be an H-pair. Then the function* $Nq\colon N \to NQJ$ *is a natural equivalence.*

This follows immediately from condition (5.1b).

In order to prove the uniqueness of the homotopy notions on $\mathcal{S}$ induced by an H-pair (Q,q) we need the following lemma

LEMMA (5.6). *Let* (Q,q) *and* (R,r) *be H-pairs and let* $K \in \mathcal{S}$. *Then the maps* $QrK\colon QK \to QRK$ *and* $RqK\colon RK \to RQK$ *are homotopy equivalences.*

The proof will be given in Section 15; use will be made of condition (5.1c).

Let (Q,q) and (R,r) be H-pairs and consider the following commutative diagram

(5.7)
$$\begin{tikzcd}
QK \arrow[r, "qQK"] \arrow[d, "rQK"] & QQK \arrow[d, "QrQK"] & \\
RQK \arrow[r, "qRQK"] & QRQK & QK \arrow[ul, "QqK"'] \arrow[dl, "QrK"] \\
RK \arrow[r, "qRK"] \arrow[u, "RqK"] & QRK \arrow[u, "QRqK"] &
\end{tikzcd}$$

It follows from Lemma (5.6) and condition (5.1b) that all maps involved in diagram (5.7) are homotopy equivalences; application of a homotopy notion $N\colon \mathcal{S}_E \to \mathcal{G}$ to this diagram thus yields a diagram in $\mathcal{G}$ consisting only of equivalences. If we put $Q = R$ and $q = r$ then it follows from the commutativity of diagram (5.7) that

$$(NQqK)^{-1} \circ NqQK = (NqQK)^{-1} \circ NQqK \circ (NQqK)^{-1} \circ NqQK = i_{NQK}.$$

Consequently

$$\begin{aligned}(NRqK)^{-1} \circ NrQK &= (NqRK)^{-1} \circ NQrK \circ (NQqK)^{-1} \circ NqQK \\ &= (NqRK)^{-1} \circ NQrK.\end{aligned}$$

Hence the following uniqueness theorem holds.

THEOREM (5.8). *Let $N\colon \mathcal{S}_E \to \mathcal{G}$ be a homotopy notion on $\mathcal{S}_E$ and let (Q, q) and (R, r) be H-pairs. Then the function $h\colon NQ \to NR$ given by*

$$hK = (NRqK)^{-1} \circ NrQK = (NqRK)^{-1} \circ NQrK$$

is a natural equivalence.

6. The simplicial singular complex of the geometrical realization. We shall now use the results of Section 5 in order to compare the simplicial singular complex of the geometrical realization of a c.s.s. complex K with $\mathrm{Ex}^\infty K$.

Let $\mathcal{A}$ be the category of topological spaces and continuous maps and let $|\ |\colon \mathcal{S} \to \mathcal{A}$ be the *geometrical realization functor* which assigns to a c.s.s. complex K its geometrical realization $|K|$ in the sense of J. Milnor (see [8]); $|K|$ is a CW-complex of which the n-cells are in one-to-one correspondence with the non-degenerate n-simplices of K.

Let $S\colon \mathcal{A} \to \mathcal{S}_E$ be the *simplicial singular functor* which assigns to a topological space X its simplicial singular complex SX (see [2]); an n-simplex of SX is any continuous map $\sigma\colon |\Delta[n]| \to X$ and for every map $\alpha\colon [m] \to [n]$ the n-simplex $\sigma\alpha$ is the composite map

$$|\Delta[m]| \xrightarrow{|\Delta\alpha|} |\Delta[n]| \xrightarrow{\sigma} X.$$

The functor S maps homotopic maps into homotopic maps.

For every c.s.s. complex K let $jK\colon K \to S|K|$ be the natural monomorphism which assigns to an n-simplex $\sigma \in K$ the simplex $|\phi\sigma|\colon |\Delta[n]|$

$\to |K|$ of $S|K|$, where $\phi_\sigma \colon \Delta[n] \to K$ is the unique c.s.s. map such that $\phi_\sigma \alpha = \sigma\alpha$ for all $\alpha \in \Delta[n]$.

The following results are due to J. Milnor ([8]).

THEOREM (6.1). *The functor* $|\ | \colon \mathcal{S} \to \mathcal{A}$ *maps homotopic maps into homotopic maps.*

COROLLARY (6.2). *The functor* $S|\ | \colon \mathcal{S} \to \mathcal{S}_E$ *maps homotopic maps into homotopic maps.*

THEOREM (6.3). *Let* $K \in \mathcal{S}_E$. *Then the map* $jK \colon K \to S|K|$ *is a homotopy equivalence.*

It is also readily verified that

THEOREM (6.4). *Let* $K \in \mathcal{S}$ *and let* $f \colon S|K| \to S|K|$ *be a c.s.s. map such that commutativity holds in the diagram*

$$\begin{tikzcd}
& S|K| \arrow[dd, "f"'] \\
K \arrow[ur, "jK"] \arrow[dr, "jK"'] & \\
& S|K|
\end{tikzcd}$$

Then f *is a homotopy equivalence.*

It follows from Corollary (6.2) and Theorems (6.3) and (6.4) that the pair $(S|\ |, j)$ is an H-pair. Application of Lemma (5.6) and Theorem (5.8) now yields

LEMMA (6.5). *Let* $K \in \mathcal{S}$. *Then the maps*

$$S|jK| \colon S|K| \to S|S|K\|, \qquad S|e^\infty K| \colon S|K| \to S|\operatorname{Ex}^\infty K|,$$

$$\operatorname{Ex}^\infty jK \colon \operatorname{Ex}^\infty K \to \operatorname{Ex}^\infty S|K|, \qquad \operatorname{Ex}^\infty e^\infty K \colon \operatorname{Ex}^\infty K \to \operatorname{Ex}^\infty \operatorname{Ex}^\infty K$$

are homotopy equivalences.

THEOREM (6.6). *Let* $N \colon \mathcal{S}_E \to \mathfrak{G}$ *be a homotopy notion on* $\mathcal{S}_E$. *Then the function* $h \colon N \operatorname{Ex}^\infty \to NS|\ |$ *given by*

$$hK = (NS|e^\infty K|)^{-1} \circ Nj \operatorname{Ex}^\infty K = (Ne^\infty S|K|)^{-1} \circ N \operatorname{Ex}^\infty jK$$

is a natural equivalence.

Theorem (6.6) asserts that the homotopy notions on $\mathcal{S}$ induced by the functor Ex^∞ are equivalent with these induced by the functor $S|\ |$. In particular we have

COROLLARY (6.7). *Let $K\in\mathcal{S}$. Then $\mathrm{Ex}^\infty K$ and $S|K|$ have the same homotopy type.*

7. Extension and subdivision. The *subdivision* of a c. s. s. complex K is a c. s. s. complex $\operatorname{Sd} K$ defined as follows. Let $\bar{K}$ denote the c. s. s. complex of which the q-simplices are pairs (σ,ξ) such that $\sigma\in K$, $\xi\in\Delta'[\dim\sigma]$ and $\dim\xi=q$, while for a map $\gamma\colon[p]\to[q]$ the p-simplex $(\sigma,\xi)\gamma$ is given by $(\sigma,\xi)\gamma=(\sigma,\xi\gamma)$. Define a relation on $\bar{K}$ by calling two simplices $(\sigma,\xi),(\tau,\rho)\in\bar{K}$ equivalent if there exists a map $\alpha\colon[\dim\tau]\to[\dim\sigma]$ such that $\tau=\sigma\alpha$ and $\xi=\Delta'\alpha(\rho)$ and let $\sim$ denote the resulting equivalence relation. Then $\operatorname{Sd} K$ is the collapsed complex $\operatorname{Sd} K=\bar{K}/(\sim)$.

A c. s. s. map $f\colon K\to L$ clearly induces a c. s. s. map $\bar{f}\colon\bar{K}\to\bar{L}$ (given by $\bar{f}(\sigma,\xi)=(f\sigma,\xi)$) which is compatible with the relation $\sim$. The *subdivision* of f then is defined as the collapsed map $\operatorname{Sd} f\colon\operatorname{Sd} K\to\operatorname{Sd} L$. Clearly the function $\operatorname{Sd}\colon\mathcal{S}\to\mathcal{S}$ so defined is a covariant functor. By $\operatorname{Sd}^n\colon\mathcal{S}\to\mathcal{S}$ we shall mean the functor Sd applied n times.

The functors Ex and Sd are closely related. With a c. s .s. map $f\colon\operatorname{Sd} K\to L$ we may associate a c. s. s. map $\beta f\colon K\to\operatorname{Ex} L$ as follows. Let $\sigma\in K$ be an n-simplex and let $c\colon\bar{K}\to\operatorname{Sd} K$ be the collapsing map. Then $(\beta f)\sigma$ is the n-simplex of $\operatorname{Ex} L$, i. e., the c. s. s. map $(\beta f)c\colon\Delta'[n]\to L$, given by $((\beta f)\sigma)\xi=(f\circ c)(\sigma,\xi)$. The function β is natural, i. e., for every two maps $a\colon K'\to K$ and $b\colon L\to L'$

$$\beta(b\circ f\circ\operatorname{Sd} a)=\operatorname{Ex} b\circ\beta f\circ a.$$

An important property of the function β is

LEMMA (7.1). *Let $K,L\in\mathcal{S}$. Then the function β establishes a one-to-one correspondence between the c. s. s. maps $\operatorname{Sd} K\to L$ and the c. s. s. maps $K\to\operatorname{Ex} L$.*

Lemma (7.1) is an immediate consequence of the results of [7]. It can also be verified by a straightforward computation

For every c. s. s. complex K define an epimorphism $dK\colon K\to K$ as follows. Let $\bar{d}K\colon\bar{K}\to K$ be the map given by

$$\bar{d}K(\sigma,\xi)=(\phi_\sigma\circ\delta[\dim\sigma])\xi,$$

where $\phi_\sigma\colon\Delta[\dim\sigma]\to K$ is the (unique) map such that $\phi_\sigma\alpha=\sigma\alpha$ for all

$\alpha \in \Delta[\dim \sigma]$. Then $\bar{d}K$ maps equivalent simplices of $\bar{K}$ into the same simplex of K and $dK\colon \operatorname{Sd} K \to K$ is defined as the map obtained by collapsing $\bar{d}K$. By $d^n K\colon \operatorname{Sd}^n K \to K$ we shall mean the composite epimorphism

$$\operatorname{Sd}^n K \xrightarrow{d(\operatorname{Sd}^{n-1} K)} \operatorname{Sd}^{n-1} K \to \cdots \to \operatorname{Sd} K \xrightarrow{dK} K$$

It is readily verified that the function d is a natural transformation $d\colon Sd \to E$.

The natural transformations $e\colon E \to \operatorname{Ex}$ and $d\colon \operatorname{Sd} \to E$ are also closely related. In fact a simple computation yields

LEMMA (7.2). *Let $K \in \mathcal{S}$. Then $\beta(dK) = eK$.*

Remark (7.3). Lemma (7.1) states that, in the terminology of [6], the functor Sd is a left adjoint of the functor Ex.

Remark (7.4). The ordered sets $[n]$ and the maps $\alpha\colon [m] \to [n]$ form a category which will be denoted by $\mathcal{V}$. The subdivided standard simplices $\Delta'[n]$ and the maps $\Delta'\alpha\colon \Delta'[m] \to \Delta'[n]$ now may be considered as the images of the objects $[n]$ and maps $\alpha\colon [m] \to [n]$ of the category $\mathcal{V}$ under a covariant functor $\Delta'\colon \mathcal{V} \to \mathcal{S}$. It then may be verified that the functors Sd and Ex may be obtained by the general method of [7], Section 3 by putting $\mathcal{Z} = \mathcal{S}$ and $\Sigma = \Delta'$.

Let $K \in \mathcal{S}$. A q-simplex of $\operatorname{Ex}^\infty K$ is a pair (σ, n) where $\sigma \in \operatorname{Ex}^n K$ is a q-simplex. As $\operatorname{Ex}^n K = \operatorname{Ex}^{n-1}(\operatorname{Ex} K)$ it follows that the pair $(\sigma, n-1)$ is a q-simplex of $\operatorname{Ex}^\infty(\operatorname{Ex} K)$. It is readily verified that this correspondence yields an isomorphism $i\colon \operatorname{Ex}^\infty K \to \operatorname{Ex}^\infty(\operatorname{Ex} K)$ such that commutativity holds in the diagram

$$\begin{tikzcd}
K \arrow[r, "e^\infty K"] \arrow[d, "eK"] & \operatorname{Ex}^\infty K \arrow[d, "i"] \\
\operatorname{Ex} K \arrow[r, "e^\infty(\operatorname{Ex} K)"] & \operatorname{Ex}^\infty(\operatorname{Ex} K)
\end{tikzcd} \tag{7.3}$$

In view of Lemma (6.5) the maps $S|e^\infty K|$ and $S|e^\infty(\operatorname{Ex} K)|$ are homotopy equivalences. Consequently the maps $|e^\infty K|$ and $|e^\infty(\operatorname{Ex} K)|$ are homotopy equivalences and it follows from the commutativity in diagram (7.3) that

LEMMA (7.4). *Let $K \in \mathcal{S}$. Then the continuous map $|eK|\colon |K| \to |\operatorname{Ex} K|$ is a homotopy equivalence.*

The following can be shown using standard methods.

LEMMA (7.5). *Let* $K \in \mathcal{S}$. *Then the continuous map* $|dK| : |\mathrm{Sd}\,K| \to |K|$ *is a homotopy equivalence.*

8. C. s. s. approximation theorems. We shall now give an exact formulation of the c. s. s. approximation theorems mentioned in the introduction.

THEOREM (8.1). *Let* $K \in \mathcal{S}$ *and let* $M \in \mathcal{S}_E$. *Then for every continuous map* $f : |K| \to |M|$ *there exists a c.s.s. map* $h : K \to M$ *such that* $|h| \simeq f$.

Let $L \in \mathcal{S}$ and let $M = \mathrm{Ex}^\infty L$. Then Theorem (8.1) implies

COROLLARY (8.2). *Let* $K, L \in \mathcal{S}$. *Then for every continuous map* $f : |K| \to |L|$ *there exists a c.s.s. map* $h : K \to \mathrm{Ex}^\infty L$ *such that the diagram*

$$\begin{tikzcd}
{|K|} \arrow[r, "f"] \arrow[dr, "{|h|}"] & {|L|} \arrow[d, "{|e^\infty L|}"] \\
 & {|\mathrm{Ex}^\infty L|}
\end{tikzcd}$$

is commutative up to homotopy, i. e., $|h| \simeq |e^\infty L| \circ f$.

Proof of Theorem (8.1). Let $\bar{j}M : S|M| \to M$ be a homotopy inverse of the map $jM : M \to S|M|$. Consider the diagram

$$\begin{tikzcd}
{|K|} \arrow[r, "{|jK|}"] \arrow[d, "f"] & {|S|K||} \arrow[d, "{|Sf|}"] & {|K|} \arrow[l, "{|jK|}"'] \arrow[d, "{|h|}"] \\
{|M|} \arrow[r, "{|jM|}"] & {|S|M||} & {|M|} \arrow[l, "{|jM|}"']
\end{tikzcd}$$

where $h : K \to M$ is the composite map

$$K \xrightarrow{jK} S|K| \xrightarrow{Sf} S|M| \xrightarrow{\bar{j}M} M.$$

Clearly commutativity holds in the rectangle at the left and the definition of h implies that the rectangle at the right is commutative up to homotopy. It follows from Lemma (6.6) that the maps $S|jK|$ and $S|jM|$ and therefore the maps $|jK|$ and $|jM|$ are homotopy equivalences. Hence $|h| \simeq f$.

A c. s. s. complex K is called *finite* if it has only a finite number of non-degenerate simplices.

THEOREM (8.3). *Let* $K, L \in \mathcal{S}$ *and let* K *be finite. Then for every continuous map* $f \colon |K| \to |L|$ *there exists an integer* $n > 0$ *and a c.s.s. map* $h \colon K \to \operatorname{Ex}^n L$ *such that the diagram*

$$\begin{tikzcd}
|K| \arrow[r, "f"] \arrow[dr, "|h|"] & |L| \arrow[d, "|e^n L|"] \\
& |\operatorname{Ex}^n L|
\end{tikzcd}$$

is commutative up to homotopy, i.e., $|h| \simeq |e^n L| \circ f$.

Proof. Application of Corollary (8.2) yields a c.s.s. map $h' \colon K \to \operatorname{Ex}^\infty L$ such that $|h'| \simeq |e^\infty L| \circ f$. As K is finite only a finite number of non-degenerate simplices of $\operatorname{Ex}^\infty L$ are in the image of K under h'. Hence there exists an integer n such that the map $h' \colon K \to \operatorname{Ex}^\infty L$ may be factorized

$$K \xrightarrow{h} \operatorname{Ex}^n L \xrightarrow{b} \operatorname{Ex}^\infty L$$

where b is the embedding map which assigns to a simplex $\sigma \in \operatorname{Ex}^n L$ the simplex $(\sigma, n) \in \operatorname{Ex}^\infty L$. By an argument similar to that used in the proof of Lemma (7.4) it follows that $|b|$ is a homotopy equivalence. The theorem now follows from the fact that the map $e^\infty L \colon L \to \operatorname{Ex}^\infty L$ may be factorized

$$L \xrightarrow{e^n L} \operatorname{Ex}^n L \xrightarrow{b} \operatorname{Ex}^\infty L.$$

In order to obtain the dual theorem, involving the functor Sd instead of Ex, we need the following lemma

LEMMA (8.4). *Let* $K, L \in \mathcal{S}$. *Then for every c.s.s. map* $h \colon K \to \operatorname{Ex} L$ *the diagram*

$$\begin{tikzcd}
|K| \arrow[r, "|h|"] & |\operatorname{Ex} L| \\
|\operatorname{Sd} K| \arrow[u, "|dK|"] \arrow[r, "|\beta^{-1} h|"] & |L| \arrow[u, "|eL|"']
\end{tikzcd}$$

is commutative up to homotopy, i.e., $|eL| \circ |\beta^{-1} h| \simeq |h| \circ |dK|$.

The proof will be given in Section 16.

Applying Lemma (8.4) n times to Theorem (8.3) we get

THEOREM (8.5). *Let $K, L \in \mathcal{S}$ and let K be finite. Then for every continuous map $f\colon |K| \to |L|$ there exists an integer $n > 0$ and a c.s.s. map $g\colon Sd^n K \to L$ such that the diagram*

$$\begin{tikzcd}
{|K|} \arrow[r, "f"] & {|L|} \\
{|\mathrm{Sd}^n K|} \arrow[u, "{|d^n K|}"] \arrow[ur, "{|g|}"'] &
\end{tikzcd}$$

is commutative up to homotopy, i.e., $|g| \simeq f \circ |d^n K|$.

Chapter II. Proofs.

9. Proof of Lemma (3.1). Let $f_0, f_1\colon K \to L \in \mathcal{S}$ be maps such that $f_0 \simeq f_1$. Using the terminology of [4] this means that there exists a c.s.s. map $f_1\colon I \times K \to L$ such that $f_I \circ \epsilon K = f_\epsilon$ ($\epsilon = 0, 1$). It is readily verified that the functor Ex commutes with the cartesian product, i.e., that for every two c.s.s. complexes A and B

$$\mathrm{Ex}(A \times B) = (\mathrm{Ex}\ A) \times (\mathrm{Ex}\, B).$$

Straightforward computation shows that commutativity holds in the diagram

$$\begin{tikzcd}
\mathrm{Ex}\, K \arrow[r, "\epsilon(\mathrm{Ex}\, K)"] \arrow[d, "\mathrm{Ex}(\epsilon K)"] & I \times (\mathrm{Ex}\, K) \arrow[d, "eI \times i_{\mathrm{Ex}\, K}"] \\
\mathrm{Ex}(I \times K) \arrow[r, "i"] & (\mathrm{Ex}\, I) \times (\mathrm{Ex}\, K)
\end{tikzcd}$$

where i is the identity. Hence

$$(\mathrm{Ex}\, f_I) \circ (eI \times i_{\mathrm{Ex}\, K}) \circ \epsilon(\mathrm{Ex}\, K) = (\mathrm{Ex}\, f_I) \circ (\mathrm{Ex}(\epsilon K)) = \mathrm{Ex}(f_I \circ \epsilon K) = \mathrm{Ex}\, f_\epsilon,$$

i.e., $(\mathrm{Ex}\, f_I) \circ (eI \times i_{\mathrm{Ex}\, K})\colon \mathrm{Ex}\, f_0 \simeq \mathrm{Ex}\, f_1$.

10. Proof of Lemma (3.2). We shall first investigate the structure of $\mathrm{Ex}\, K$.

A map $\alpha\colon [m] \to [n]$ was defined as a monotone function. By a *function* $\zeta\colon [m] \to [n]$ we shall mean merely a function which thus need not be monotone. A *permutation* $\pi\colon [m] \to [m]$ is a function which is one-to-one onto.

Let $\pi\colon [m] \to [m]$ be a permutation. Then π induces an automorphism $\pi'\colon \Delta'[m] \to \Delta'[m]$ as follows. For each map $\sigma\colon [q] \to [m]$ let $\sigma^{\pi}\colon [q] \to [m]$ be a map and let $\phi\colon [q] \to [q]$ be a permutation such that commutativity holds in the diagram

$$\begin{tikzcd}
{[q]} \arrow[r, "\sigma"] \arrow[d, "\phi"] & {[m]} \arrow[d, "\pi"] \\
{[q]} \arrow[r, "\sigma^{\pi}"] & {[m]}
\end{tikzcd}$$

Clearly such a map σ^{π} and permutation ϕ exist. It is easily seen that

(a) σ^{π} is unique;

(b) if σ is a monomorphism, then so is σ^{π};

(c) if σ lies on τ, then σ^{π} lies on τ^{π}.

We now define the automorphism $\pi'\colon \Delta'[m] \to \Delta'[m]$ by

$$\pi'(\sigma_0, \cdots, \sigma_q) = (\sigma_0{}^{\pi}, \cdots, \sigma_q{}^{\pi}).$$

Let $\zeta\colon [m] \to [n]$ be a function. Then ζ induces a c. s. s. map $\zeta'\colon \Delta'[m] \to \Delta'[n]$ as follows. There clearly exists a permutation $\pi\colon [m] \to [m]$ and a unique map $\alpha\colon [m] \to [n]$ such that commutativity holds in the diagram

$$\begin{tikzcd}
{[m]} \arrow[d, "\pi"] \arrow[rd, "\zeta"] & \\
{[m]} \arrow[r, "\alpha"] & {[n]}
\end{tikzcd}$$

The c. s. s. map $\zeta'\colon \Delta'[m] \to \Delta'[n]$ is now defined as the composite map

$$\Delta'[m] \xrightarrow{\pi'} \Delta'[m] \xrightarrow{\Delta'\alpha} \Delta'[n].$$

It is readily verified that

(a) the c. s. s. map ζ' is independent of the choice of the permutation π;

(b) if ζ is a permutation, then this definition of ζ' coincides with the above one;

(c) if ζ is a map, then $\zeta' = \Delta'\zeta$;

(d) if $\vartheta\colon [l] \to [m]$ is a function, then $(\zeta\vartheta)'$ is the composite map;

$$\Delta'[l] \xrightarrow{\vartheta'} \Delta'[m] \xrightarrow{\zeta'} \Delta'[n].$$

$\operatorname{Ex} K$ is a c. s. s. complex. This means that for every n-simplex $\sigma \in \operatorname{Ex} K$ and every *map* $\alpha : [m] \to [n]$ there is given an m-simplex $\sigma\alpha \in \operatorname{Ex} K$ such that

(i) $\sigma\epsilon_n = \sigma$ where $\epsilon_n : [n] \to [n]$ is the identity;

(ii) if $\beta : [l] \to [m]$ is a map, then $(\sigma\alpha)\beta = \sigma(\alpha\beta)$.

Now let $\sigma \in \operatorname{Ex} K$ be an n-simplex and let $\zeta : [m] \to [n]$ be a *function.* Then the composite map

$$\Delta'[m] \xrightarrow{\zeta'} \Delta'[n] \xrightarrow{\sigma} K$$

is an m-simplex of $\operatorname{Ex} K$ which will be denoted by $\sigma\zeta$. If $\vartheta : [l] \to [m]$ is also a function, then clearly $(\sigma\zeta)\vartheta = \sigma(\zeta\vartheta)$. Thus $\operatorname{Ex} K$ *has more structure than a c.s.s. complex.* It is this additional structure which will be used in the proof of Lemma (3.2).

Proof of Lemma (3.2). Let $\Lambda \subset \Delta[n]$ be the subcomplex generated by the non-degenerate $(n-1)$-simplices $\epsilon^0, \cdots, \epsilon^{k-1}, \epsilon^{k+1}, \cdots, \epsilon^n$ and let $\lambda : \Lambda \to \operatorname{Ex} K$ be the c. s. s. map such that $\lambda\epsilon^i = \tau_i$. Then we must define a c. s. s. map $\rho : \Delta'[n] \to \operatorname{Ex} K$ such that for each $i \neq k$ commutativity holds in the diagram

$$\begin{tikzcd}
\Delta'[n-1] \arrow[r, "\Delta'\epsilon^i"] \arrow[d, "{\delta[n-1]}"] & \Delta'[n] \arrow[dr, "\rho"] & \\
 & & \operatorname{Ex} K \\
\Delta[n-1] \arrow[r, "\Delta\epsilon^i"] & \Lambda \arrow[ur, "\lambda"'] &
\end{tikzcd} \tag{10.1}$$

For each simplex $(\sigma_0, \cdots, \sigma_q) \in \Delta'[n]$ define a function $\zeta(\sigma_0, \cdots, \sigma_q) : [q] \to [n]$ by

$$\zeta(\sigma_0, \cdots, \sigma_q)(i) = \sigma_i(\dim \sigma_i), \qquad \sigma_i \neq \epsilon^k \text{ or } \epsilon_n$$

$$\zeta(\sigma_0, \cdots, \sigma_q)(i) = k, \qquad \sigma_i = \epsilon^k \text{ or } \epsilon_n.$$

Then there exists a permutation $\phi : [q] \to [q]$ and a unique map $\sigma : [q] \to [n]$ such that commutativity holds in the diagram

$$\begin{tikzcd}
{[q]} \arrow[d, "\phi"] \arrow[dr, "{\zeta(\sigma_0, \cdots, \sigma_q)}"] & \\
{[q]} \arrow[r, "\sigma"] & {[n]}
\end{tikzcd}$$

It is easily seen that $\sigma \in \Lambda$. We now define $\rho(\sigma_0, \cdots, \sigma_q) = (\lambda\sigma)\phi$. It may be verified by direct computation that this definition is independent of the choice of the permutation ϕ.

We now show that the function $\rho\colon \Delta'[n] \to \operatorname{Ex} K$ so defined is a c. s. s. map. Let $\beta\colon [p] \to [q]$ be a map. Then there exists a permutation $\psi\colon [p] \to [p]$ and a unique map $\gamma\colon [p] \to [q]$ such that commutativity holds in the diagram

$$\begin{tikzcd}
{[p]} \arrow[r, "\beta"] \arrow[d, "\psi"'] & {[q]} \arrow[d, "\phi"] \arrow[dr, "\zeta(\sigma_0, \cdots, \sigma_q)"] & \\
{[p]} \arrow[r, "\gamma"] & {[q]} \arrow[r, "\sigma"] & {[n]}
\end{tikzcd}$$

The function $\zeta((\sigma_0, \cdots, \sigma_q)\beta)$ is the composite function

$$[p] \xrightarrow{\beta} [q] \xrightarrow{\zeta(\sigma_0, \cdots, \sigma_q)} [n]$$

and consequently $\rho((\sigma_0, \cdots, \sigma_q)\beta) = (\lambda(\sigma\gamma))\psi$. As commutativity also holds in the diagram

$$\begin{tikzcd}
\Delta'[p] \arrow[r, "\Delta'\beta"] \arrow[d, "\psi'"] & \Delta'[q] \arrow[d, "\phi'"] & \\
\Delta'[p] \arrow[r, "\Delta'\gamma"] & \Delta'[q] \arrow[r, "\lambda\sigma"] & K
\end{tikzcd}$$

it follows that

$$\lambda(\sigma\gamma))\psi = \lambda\sigma \circ \Delta'\gamma \circ \psi' = \lambda\sigma \circ \phi' \circ \Delta'\beta = ((\lambda\sigma)\pi)\beta$$

i. e., the function $\rho\colon \Delta'[n] \to \operatorname{Ex} K$ is a c. s. s. map.

It thus remains to show that commutativity holds in diagram (10. 1). Let $(\tau_0, \cdots, \tau_q) \in \Delta'[n-1]$. Then

$$\Delta'\epsilon^i(\tau_0, \cdots, \tau_q) = (\epsilon^i\tau_0, \cdots, \epsilon^i\tau_q).$$

If $i \neq k$, then clearly $\epsilon^i\tau_j \neq \epsilon^k$ and $\epsilon^i\tau_j \neq \epsilon_n$ for all j and it follows from the definitions of the maps ρ and $\delta[n]$ that

$$(\rho \circ \Delta'\epsilon^i)(\tau_0, \cdots, \tau_q) = (\lambda \circ \delta[n] \circ \Delta'\epsilon^i)(\tau_0, \cdots, \tau_q).$$

Application of Lemma (2.2) now yields

$$(\rho\circ\Delta'\epsilon^i)(\tau_0,\cdots,\tau_q)=(\lambda\circ\Delta\epsilon^i\circ\delta[n-1])(\tau_0,\cdots,\tau_q).$$

This completes the proof.

11. Proof of Lemma (3.4).

Let k be an integer with $0\leqq k\leqq n$, let $\tau_0,\cdots,\tau_{k-1},\tau_{k+1},\cdots,\tau_n\in\operatorname{Ex}K$ be n $(n-1)$-simplices such that $\tau_i\epsilon^{j-1}=\tau_j\epsilon^i$ for $i<j$ and $i\neq k\neq j$ and let $\rho\in\operatorname{Ex}L$ be an n-simplex such that $(\operatorname{Ex}f)\tau_i=\rho\epsilon^i$ for $i=0,\cdots,\hat{k},\cdots,n$. Then in order to prove the first part of Lemma (3.4) we must show that there exists a c.s.s. map $\tau\colon\Delta'[n]\to K$ such that for each integer $i\neq k$ commutativity holds in the diagram

(11.1)
$$\begin{tikzcd}
\Delta'[n-1] \arrow[r, "\tau_i"] \arrow[d, "\Delta'\epsilon^i"'] & K \arrow[d, "f"] \\
\Delta'[n] \arrow[r, "\rho"] \arrow[ur, "\tau"] & L
\end{tikzcd}$$

For each simplex $(\sigma_0,\cdots,\sigma_q)\in\Delta'[n]$ for which there exists an integer $i\neq k$ and a simplex $(\sigma_0{}^i,\cdots,\sigma_q{}^i)\in\Delta'[n-1]$ such that $\Delta'\epsilon^i(\sigma_0{}^i,\cdots,\sigma_q{}^i)=(\sigma_0,\cdots,\sigma_q)$ define

$$\tau(\sigma_0,\cdots,\sigma_q)=\tau_i(\sigma_0{}^i,\cdots,\sigma_q{}^i).$$

This definition is independent of the choice of i. If j is another such integer and $i<j$ then there exists a simplex $(\sigma_0{}^{ij},\cdots,\sigma_q{}^{ij})\in\Delta'[n-2]$ such that $\Delta'\epsilon^{j-1}(\sigma_0{}^{ij},\cdots,\sigma_q{}^{ij})=(\sigma_0{}^i,\cdots,\sigma_q{}^i)$ and $\Delta'\epsilon^i(\sigma_0{}^{ij},\cdots,\sigma_q{}^{ij})=(\sigma_0{}^j,\cdots,\sigma_q{}^j)$.

Hence

$$\begin{aligned}\tau_i(\sigma_0{}^i,\cdots,\sigma_q{}^i)&=\tau_i(\Delta'\epsilon^{j-1}(\sigma_0{}^{ij},\cdots,\sigma_q{}^{ij}))=\tau_i\epsilon^{j-1}(\sigma_0{}^{ij},\cdots,\sigma_q{}^{ij})\\&=\tau_j\epsilon^i(\sigma_0{}^{ij},\cdots,\sigma_q{}^{ij})=\tau_j(\Delta'\epsilon^i(\sigma_0{}^{ij},\cdots,\sigma_q{}^{ij}))=\tau_j(\sigma_0{}^j,\cdots,\sigma_q{}^j).\end{aligned}$$

It is readily verified that the function τ so defined on all simplices of $\Delta'[n]$ which are in the image of $\Delta'[n-1]$ under a map $\Delta'\epsilon^i$ with $i\neq k$, (i.e., those simplices $(\sigma_0,\cdots,\sigma_q)\in\Delta'[n]$ for which $\sigma_q\neq\epsilon_n$ or ϵ^k), commutes with all operators $\beta\colon[p]\to[q]$ and is such that commutativity holds in the upper left triangle of diagram (11.1).

It thus remains to show that τ can be extended over all of $\Delta'[n]$ (i.e., over the simplices $(\sigma_0,\cdots,\sigma_q)\in\Delta'[n]$ for which $\sigma_q=\epsilon_n$ or ϵ^k) to a c.s.s.

map in such a manner that commutativity also holds in the lower right triangle of diagram (11.1). For each non-degenerate simplex $(\sigma_0,\cdots,\sigma_q)$ with $\sigma_q=\epsilon_n$ let $T(\sigma_0,\cdots,\sigma_q)$ denote the triple (l,m,q) where l is the smallest integer such that $\sigma_l(i)=k$ for some i and $m=\dim\sigma_l$. Order these triples lexicographically. It is readily verified that

(i) if $T(\sigma_0,\cdots,\sigma_q)=(l,m,q)$ and $\dim_{l-1}<m-1$ or $l=0, m>0$, then there exists a simplex $(\sigma_0',\cdots,\sigma_{q+1}')\in\Delta'[n]$ such that $(\sigma_0',\cdots,\sigma_{q+1})\epsilon^l=(\sigma_0,\cdots,\sigma_q)$ and $T(\sigma_0',\cdots,\sigma_{q+1}')=(l,m-1,q+1)<(l,m,q)$.

(ii) if $T(\sigma_0,\cdots,\sigma_q)=(l,m,q)$ and $\dim\sigma_{l-1}=m-1, l<q$ or $l=m=0$, then (a) $T((\sigma_0,\cdots,\sigma_q)\epsilon^i)<(l,m,q)$ for $i\neq l,q$, (b) $\sigma_{q-1}\neq\epsilon^k$ and hence $\tau((\sigma_0,\cdots,\sigma_q)\epsilon^q)$ has already been defined, (c) $T((\sigma_0,\cdots,\sigma_q)\epsilon^l)>(l,m,q)$ and (d) if $T(\sigma_0',\cdots,\sigma_q')\leqq(l,m,q)$, then $(\sigma_0,\cdots,\sigma_q)\epsilon^l$ is not a face of $(\sigma_0',\cdots,\sigma_q')$.

(iii) if $T(\sigma_0,\cdots,\sigma_q)=(q,n,q)$ and $\dim\sigma_{l-1}=n-1$, then (a) $T((\sigma_0,\cdots,\sigma_q)\epsilon^i)<(q,n,q)$ for $i\neq q$, (b) $\sigma_{q-1}=\epsilon^k$ and (c) if $T(\sigma_0',\cdots,\sigma_q')\leqq(q,n,q)$, then $(\sigma_0,\cdots,\sigma_{q-1})$ is not a face of $(\sigma_0',\cdots,\sigma_q')$.

We now extend τ as follows. Let (l,m,q) be a triple and suppose that τ has already been extended over all non-degenerate simplices $(\sigma_0,\cdots,\sigma_{q-1},\epsilon_n)$ and their faces for which $T(\sigma_0,\cdots,\sigma_{q-1},\epsilon_n)<(l,m,q)$ and over some non-degenerate simplices $(\sigma_0,\cdots,\sigma_{q-1},\epsilon_n)$ and their faces for which $T(\sigma_0,\cdots,\sigma_{q-1},\epsilon_n)=(l,m,q)$ in such a manner that τ commutes with all face operators and that commutativity holds in the lower right triangle of diagram (11.1). Let $(\sigma_0,\cdots,\sigma_{q-1},\epsilon_n)$ be a non-degenerate simplex such that $T(\sigma_0,\cdots,\sigma_{q-1},\epsilon_n)=(l,m,q)$ and on which τ has not yet been defined. It then follows from (i) that $\dim\sigma_{l-1}=m-1$ or $l=m=0$ and from (ii) or (iii) that τ already has been defined on all faces of $(\sigma_0,\cdots,\sigma_{q-1},\epsilon_n)$ except $(\sigma_0,\cdots,\sigma_{q-1},\epsilon_n)\epsilon^l$. Because f is a fibre map there exists a q-simplex $\psi\in K$ such that

$$\rho(\sigma_0,\cdots,\sigma_{q-1},\epsilon_n)=f\psi,\qquad \tau((\sigma_0,\cdots,\sigma_{q-1},\epsilon_n)\epsilon^i)=\psi\epsilon^i\qquad(i\neq k).$$

Now define

$$\tau(\sigma_0,\cdots,\sigma_{q-1},\epsilon_n)=\psi,\qquad \tau((\sigma_0,\cdots,\sigma_{q-1},\epsilon_n)\epsilon^l)=\psi\epsilon^l.$$

It is readily verified that the function τ so extended commutes with all face operators and is such that commutativity holds in the lower right triangle of diagram (11.1). Thus using induction on the triples (l,m,q) τ may be extended over all non-degenerate simplices $(\sigma_0,\cdots,\sigma_{q-1},\epsilon_n)\in\Delta'[n]$ and their faces. As every non-degenerate simplex $(\sigma_0,\cdots,\sigma_{q-2},\epsilon^k)\in\Delta'[n]$ is a face of a non-degenerate simplex $(\sigma_0, \cdots, \sigma_{q-2}, \epsilon^k, \epsilon_n)$ it follows that τ may be extended over all non-degenerate simplices of $\Delta'[n]$ in such a manner that τ commutes with all face operators and that commutativity holds in diagram (11.1). Extensions of τ over the degenerate simplices of $\Delta'[n]$ (which is always possible in a unique way) now yields the desired c. s. s. map τ: $\Delta'[n] \rightarrow K$.

The second part of Lemma (3.4) is obvious.

12. Proof of Lemma (3.6). We shall use the theory of acyclic models of Eilenberg-MacLane (see [1]). The models will be the complexes $\Delta[n]$ and $\Delta'[n]$. Let C_a: $\mathcal{S} \rightarrow \partial\mathcal{G}$ be the augmented chain functor. As the map eK: $K \rightarrow \operatorname{Ex} K$ induces a one-to-one correspondence between the 0-simplices of K and those of $\operatorname{Ex} K$ it is sufficient to prove that

(a) the functor C_a: $\mathcal{S} \rightarrow \partial\mathcal{G}$ is representable in dimension > 0,

(b) the composite functor $\mathcal{S} \xrightarrow{\operatorname{Ex}} \mathcal{S} \xrightarrow{C_a} \partial\mathcal{G}$ is representable in dimension > 0, and

(c) for every integer $n \geqq 0$,

$$H_*(\Delta[n]) = H_*(\operatorname{Ex} \Delta[n]) = 0, \qquad H_*(\Delta'[n]) = H_*(\operatorname{Ex} \Delta'[n]) = 0.$$

Let $K \in \mathcal{S}$, for every n-simplex $\sigma \in K$ let ϕ_σ: $\Delta[n] \rightarrow K$ be the unique c. s. s. map such that $\phi_\sigma \alpha = \sigma\alpha$ for all $\alpha \in \Delta[n]$ and let ϵ_n' be the generator of $C_a\Delta[n]$ corresponding to the identity map ϵ_n: $[n] \rightarrow [n]$, i. e., the only non-degenerate n-simplex of $\Delta[n]$. Then it is easily seen that the function $\sigma \rightarrow (\sigma, \epsilon_n')$ yields a representation of the functor C_a.

Let $K \in \mathcal{S}$, let τ: $\Delta'[n] \rightarrow K$ be an n-simplex of $\operatorname{Ex} K$ and let ι_n' be the generator of $C_a \operatorname{Ex} \Delta'[n]$ corresponding with the identity map ι_n: $\Delta'[n] \rightarrow \Delta'[n]$. Then it is easily seen that the function $\tau \rightarrow (\tau, \iota_n')$ yields a representation of the functor $C_a\operatorname{Ex}$.

For every integer $n \geqq 0$ the (unique) map $\Delta[n] \rightarrow \Delta[0]$ is a homotopy equivalence in $\mathcal{S}$. Combining this with Lemma (3.1) and the fact that $\Delta[0] \approx \operatorname{Ex} \Delta[0]$ and $H_*(\Delta[0]) = 0$ we get $H_*(\Delta[n]) = H_*(\operatorname{Ex} \Delta[n]) = 0$. If for each integer $n \geqq 0$ the map $\delta[n]$: $\Delta'[n] \rightarrow \Delta[n]$ is a homotopy equivalence, then $H_*(\Delta'[n]) = H_*(\Delta[n]) = 0$, and Lemma (3.1) implies $H_*(\operatorname{Ex} \Delta'[n]) = H_*(\operatorname{Ex} \Delta[n]) = 0$. It thus remains to show that $\delta[n]$ is a homotopy equivalence.

For each integer i with $0 \leqq i \leqq n$ let β_i: $[i] \rightarrow [n]$ be the map given by $\beta_i(j) = j$, $0 \leqq j \leqq i$. Define a function $\delta'[n]$: $\Delta[n] \rightarrow \Delta'[n]$ by $\delta[n]\sigma = (\beta_{\sigma(0)}, \cdots, \beta_{\sigma(q)})$, $\dim \sigma = q$. As for every map α: $[p] \rightarrow [q]$,

$$(\delta'[n]\sigma)\alpha = (\beta_{\sigma(0)}, \cdots, \beta_{\sigma(q)}\alpha = (\beta_{\sigma\alpha(0)}, \cdots, \beta_{\sigma\alpha(p)}) = \delta'[n](\sigma\alpha),$$

it follows that $\delta'[n]$ is a c. s. s. map. The composite map

$$\begin{tikzcd} \Delta[n] \arrow[r, "{\delta'[n]}"] & \Delta'[n] \arrow[r, "{\delta[n]}"] & \Delta[n] \end{tikzcd}$$

is the identity because for $\sigma \in \Delta[n]$ and $0 \leqq i \leqq \dim \sigma$

$$(\delta[n]\delta'[n]\sigma)(i) = \beta_{\sigma(i)}(\sigma(i)) = \sigma(i).$$

It thus remains to prove that the composite map

$$\begin{tikzcd} \Delta'[n] \arrow[r, "{\delta[n]}"] & \Delta[n] \arrow[r, "{\delta'[n]}"] & \Delta'[n] \end{tikzcd}$$

is homotopic with the identity $\iota_n \colon \Delta'[n] \rightarrow \Delta'[n]$.

For each simplex $\sigma \in \Delta[n]$, let $\bar{\sigma} = \beta_{\sigma(\dim \sigma)}$. Define a function h: $\Delta[1] \times \Delta'[n] \rightarrow \Delta'[n]$ by

$$h(\epsilon^0\eta^0 \cdots \eta^{q-1}, (\sigma_0, \cdots, \sigma_q)) = (\bar{\sigma}_0, \cdots, \bar{\sigma}_q),$$

$$h(\epsilon^1\eta^0 \cdots \eta^{q-1}, (\sigma_0, \cdots, \sigma_q)) = (\sigma_0, \cdots, \sigma_q),$$

$$h(\epsilon_1\eta^0 \cdots \eta^{i-1}\eta^{i+1} \cdots \eta^{q-1}, (\sigma_0, \cdots, \sigma_q)) = (\sigma_0, \cdots, \sigma_i, \bar{\sigma}_{i+1}, \cdots, \bar{\sigma}_q).$$

A straightforward computation shows that the function h so defined is a c. s. s. map. It is now easily verified that h is the required homotopy.

13. Proof of Lemma (3.7). Use will be made of the following c. s. s. analogues of two theorems of J. H. C. Whitehead ([10]).

THEOREM (13.1). *Let* $K, L \in \mathcal{S}_E$ *be connected and let* $\phi \in K$ *be a* 0*-simplex. Then a c. s. s. map* $f \colon K \rightarrow L$ *is a homotopy equivalence if and only if* f *induces isomorphisms of all homotopy groups, i. e.,* $f_* \colon \pi_n(K; \phi) \approx \pi_n(L; f\phi)$, $n \geqq 1$.

THEOREM (13.2). *Let* $K, L \in \mathcal{S}_E$ *be simply connected. Then a c. s. s. map* $f \colon K \rightarrow L$ *is a homotopy equivalence if and only if* f *induces isomorphisms of all homology groups, i. e.,* $f_* \colon H_*(K) \approx H_*(L)$.

We also need the following lemma

LEMMA (13.3). *Let* $K \in \mathcal{S}_E$ *and let* $\phi \in K$ *be a* 0*-simplex. Then* $(eK)_* \colon \pi_1(K; \phi) \approx \pi_1(\operatorname{Ex} K; (eK)\phi)$.

Proof of Lemma (3.7). In this proof we shall freely use the results of [9] Clearly K may be supposed to be minimal. Let $\pi = \pi_1(K)$. Then there exists a fibre map $p\colon K \to K(\pi, 1)$ with simply connected fibre F. Let $q\colon F \to K$ be the inclusion map, then it follows from the naturality of e that commutativity holds in the diagram

$$\begin{tikzcd}
F \arrow[r, "q"] \arrow[d, "eF"] & K \arrow[r, "p"] \arrow[d, "eK"] & K(\pi, 1) \arrow[d, "e(K(\pi, 1))"] \\
\mathrm{Ex}\, F \arrow[r, "\mathrm{Ex}\, q"] & \mathrm{Ex}\, K \arrow[r, "\mathrm{Ex}\, p"] & \mathrm{Ex}\, K(\pi, 1)
\end{tikzcd}$$

By Lemma (3.4) $\mathrm{Ex}\, p$ is a fibre map with $\mathrm{Ex}\, F$ as a fibre. Hence in order to prove that eK is a homotopy equivalence it is, in view of the exactness of the homotopy sequence of a fibre map, the "five lemma" and Theorem (13.1), sufficient to prove that eF and $e(K(\pi, 1))$ are homotopy equivalences.

As F is simply connected, so is $\mathrm{Ex}\, F$ (Lemma (13.3)). Hence it follows from Lemma (3.6) and Theorem (13.2) that eF is a homotopy equivalence.

There exists a fibre map $t\colon W(K(\pi, 0)) \to K(\pi, 1)$ with $K(\pi, 0)$ as fibre and, as above, in order to prove that $e(K(\pi, 1))$ is a homotopy equivalence it suffices to prove that $e(W(K(\pi, 0)))$ and $e(K(\pi, 0))$ are so. As $W(K(\pi, 0))$ is contractible and a fortiori simply connected the argument applied to F yields that $e(W(K(\pi, 0)))$ is a homotopy equivalence. It is also readily verified that $e(K(\pi, 0))$ is an isomorphism. Hence $e(K(\pi, 1))$ is a homotopy equivalence.

This completes the proof of Lemma (3.7).

Proof of Lemma (13.3). For a definition of the fundamental group see [9].

Let $\sigma \in \Delta[n]$ be a non-degenerate q-simplex, i.e., the map $\sigma\colon [q] \to [n]$ is a monomorphism. Then σ is completely determined by the set $(\sigma(0), \cdots, \sigma(q))$, the image of $[q]$ under σ. We shall often write $(\sigma(0), \cdots, \sigma(q))$ instead of σ.

We first prove that $(eK)_*\colon \pi_1(K; \phi) \to \pi_1(\mathrm{Ex}\, K; (eK)\phi)$ is a monomorphism. Let $a \in \pi_1(K; \phi)$ be such that $(eK)_* a = 1$ and let $\tau \in a$. Then there exists a 2-simplex $\rho \in \mathrm{Ex}\, K$ such that $\rho\epsilon^2 = (eK)\tau$ and $\rho\epsilon^0 = \rho\epsilon^1 = (eK)\phi\eta^0$. Iterated application of the extension condition yields 4 3-simplices $\tau_1, \tau_3, \tau_2, \tau_4 \in K$ such that

$$\tau_1\epsilon^1 = \rho((1), (0,1), (0,1,2)); \quad \tau_1\epsilon^2 = \rho((1), (1,2), (0,1,2)); \quad \tau_1\epsilon^3 = \phi\eta^0\eta^0$$

$$\tau_2\epsilon^0 = \tau_1\epsilon^0; \quad \tau_2\epsilon^2 = \rho((2), (1,2), (0,1,2)); \quad \tau_2\epsilon^3 = \phi\eta^0\eta^0$$

$$\tau_3\epsilon^1 = \tau_2\epsilon^1; \quad \tau_3\epsilon^2 = \rho((2),(0,2),(0,1,2)); \quad \tau_3\epsilon^3 = \phi\eta^0\eta^0$$

$$\tau_4\epsilon^0 = \tau_3\epsilon^0; \quad \tau_4\epsilon^1 = \rho((0),(0,1),(0,1,2)); \quad \tau_4\epsilon^2 = \rho((0),(0,2),(0,1,2)).$$

Then

$$\tau_4\epsilon^3\epsilon^0 = \tau_4\epsilon^0\epsilon^2 = \tau_3\epsilon^0\epsilon^2 = \tau_3\epsilon^3\epsilon^0 = \phi\eta^0$$

$$\tau_4\epsilon^3\epsilon^1 = \tau_4\epsilon^0\epsilon^2 = \rho((0),(0,1)) = \sigma$$

$$\tau_4\epsilon^3\epsilon^2 = \tau_4\epsilon^2\epsilon^2 = \rho((0),(0,2)) = \phi\eta^0.$$

Consequently $a = 1$.

We now show that $(ek)_*: \pi_1(K;\phi) \to \pi_1(\operatorname{Ex} K; (eK)\phi)$ is an epimorphism. Let $\psi \in b \in \pi_1(\operatorname{Ex} K; (eK)\phi)$. Define a c. s. s. map $\rho: \Delta'[2] \to K$ by $\rho((0),(0,1)) = \psi((0),(0,1))$, $\rho((1),(0,1)) = \psi((1),(0,1))$,

$$\rho((1),(1,2),(0,1,2)) = \rho((2),(0,2),(0,1,2)) = \rho((2),(1,2),(0,1,2)) = \phi\eta^0\eta^0,$$

and extend ρ over $((0),(0,1),(0,1,2))$, $((0),(0,2),(0,1,2))$ and $((1),(0,1),(0,1,2))$ by iterated application of the extension condition. Then

$$\rho\epsilon^0 = (eK)\phi\eta^0, \qquad \rho\epsilon^1 = (eK)\rho((0),(0,2)), \qquad \rho\epsilon^2 = \tau$$

Consequently there exists an element $a \in \pi_1(K,\phi)$ such that $\rho((0),(0,2)) \in a$ and $(eK)_* a = b$.

14. Proof of Theorem (4.6). Clearly K may suppose to be connected. Let $\phi \in \operatorname{Ex}^\infty K$ be a 0-simplex, then in view of Theorem (13.1) it suffices to prove that $f_*: \pi_n(\operatorname{Ex}^\infty K;\phi) \approx \pi_n(\operatorname{Ex}^\infty K; f\phi)$ for all $n \geqq 1$. We shall only give a proof for $n = 1$. The proof for $n > 1$ is similar although more complicated.

Let $a \in \pi_1(\operatorname{Ex}^\infty K;\phi)$ and let τ be a representant of a. Suppose there exists a 2-simplex $\rho \in \operatorname{Ex}^\infty K$ such that

$$(14.1) \qquad \rho\epsilon^0 = \tau\epsilon^0\eta^0, \qquad \rho\epsilon^1 = \tau, \qquad \rho\epsilon^2 = f\tau.$$

Then clearly $f_* a = a$. Hence it suffices to show that for every 1-simplex $\tau \in \operatorname{Ex}^\infty K$ there exists a 2-simplex $\rho \in \operatorname{Ex}^\infty K$ satisfying condition (14.1).

Let $\tau \in \operatorname{Ex}^\infty K$ be a 1-simplex and let n be the smallest integer $n \geqq 0$ such that $\tau = (\psi, n)$ (by $\tau = (\psi, 0)$ we mean $\tau = (e^\infty K)\psi$). If $n = 0$, then by hypothesis $\rho = \tau\eta^1$ is the desired 2-simplex. Now suppose it has already been proved that if $n < m$, then there exists a 2-simplex ρ satisfying (14.1a). Then we must show that this is also the case if $n = m$.

Define, using the notation of Section 13, a 2-simplex $\vartheta \in \operatorname{Ex}^n K$ as follows.

$$\vartheta((0),(0,1),(0,1,2))=\vartheta((0),(0,2),(0,1,2))=\psi((0),(0,1))\eta^1$$
$$\vartheta((1),(0,1),(0,1,2))=\vartheta((1),(1,2),(0,1,2))=\psi((1),(0,1))\eta^1$$
$$\vartheta((2),(0,2),(0,1,2))=\vartheta((2),(1,2),(0,1,2))=\psi((0,1))\eta^0\eta^1.$$

Then it is readily verified that

$$\vartheta\epsilon^0=(e(\mathrm{Ex}^{n-1}K))\psi((1),(0,1)),\qquad \vartheta\epsilon^1=(e(\mathrm{Ex}^{n-1}K))\psi((0),(0,1)),\qquad \vartheta\epsilon^2=\psi.$$

By the induction hypothesis there exist 2-simplices $\rho_0,\rho_1\in\mathrm{Ex}^\infty K$ such that

$$\rho_0\epsilon^0=(\psi((0,1))\eta^0,n-1),\qquad \rho_0\epsilon^1=(\vartheta\epsilon^0,n),\qquad \rho_0\epsilon^2=f(\vartheta\epsilon^0,n)$$
$$\rho_1\epsilon^0=(\psi((0,1))\eta^0,n-1),\qquad \rho_1\epsilon^1=(\vartheta\epsilon^1,n),\qquad \rho_1\epsilon^2=f(\vartheta\epsilon^1,n).$$

Application of the extension condition then yields 3-simplices $\kappa,\lambda\in\mathrm{Ex}^\infty K$ such that

$$\kappa\epsilon^0=\rho_0,\quad \kappa\epsilon^1=\rho_1,\quad \kappa\epsilon^3=f(\vartheta,n),$$
$$\lambda\epsilon^0=(\vartheta\epsilon^0\eta^0,n),\quad \lambda\epsilon^1=(\vartheta,n),\quad \lambda\epsilon^2=\kappa\epsilon^2.$$

It then follows by direct computation that $\lambda\epsilon^3$ is the desired 2-simplex, i.e.,

$$\lambda\epsilon^3\epsilon^0=\tau\epsilon^0\eta^0,\quad \lambda\epsilon^3\epsilon^1=\tau,\quad \lambda\epsilon^3\epsilon^2=f\tau.$$

15. Proof of Lemma (5.7). Consider the commutative diagram

$$\begin{tikzcd}
& QK \arrow[dl, "rQK"'] \arrow[dr, "QrK"] & \\
RQK & K \arrow[u, "qK"'] \arrow[d, "rK"] & QRK \\
& RK \arrow[ul, "RqK"] \arrow[ur, "qRK"'] &
\end{tikzcd}$$

It follows from Definition (5.1b) that the maps rQK and qRK are homotopy equivalences. Let αK (resp. βK) be a homotopy inverse of rQK (resp. qRK). Then the following diagram is commutative up to homotopy

$$\begin{tikzcd}
& QK \arrow[dr, "QrK"] & \\
RQK \arrow[ur, "\alpha K"] & K \arrow[u, "qK"'] \arrow[d, "rK"] & QRK \arrow[dl, "\beta K"] \\
& RK \arrow[ul, "RqK"] &
\end{tikzcd}$$

i.e., $qK \simeq \alpha K \circ RqK \circ rK$ and $rK \simeq \beta K \circ QrK \circ qK$. Consequently

$$qK \simeq (\alpha K \circ RqK) \circ (\beta K \circ QrK) \circ qK,$$
$$rK \simeq (\beta K \circ QrK) \circ (\alpha K \circ RqK) \circ rK.$$

Application of the homotopy extension theorem (which holds for objects of $\mathcal{S}_E$; see [9]) yields c. s. s. maps $s\colon QK \to QK$, $t\colon RK \to RK$ such that

$$s \simeq (\alpha K \circ RqK) \circ (\beta K \circ QrK), \qquad t \simeq (\beta K \circ QrK) \circ (\alpha K \circ RqK)$$

and

$$s(qK)\sigma = (qK)\sigma, \qquad t(rK)\sigma = (rK)\sigma$$

for every simplex $\sigma \in K$. It then follows from condition (5.1c) that s and t are homotopy equivalences. Thus $\alpha K \circ RqK$ and $\beta K \circ QrK$ are homotopy equivalences and because αK and βK are also homotopy equivalences, so are RqK and QrK.

16. Proof of Lemma (8.4). Let $i_{\mathrm{Ex}\,L}\colon L \to \mathrm{Ex}\,L$ be the identity map and let $\mu L = \beta^{-1} i_{\mathrm{Ex}\,L}$. Consider the diagram

$$\begin{tikzcd}
\lvert K \rvert \arrow[dd, "\lvert h \rvert"'] & & & \lvert \mathrm{Sd}\,K \rvert \arrow[lll, "\lvert dK \rvert"'] \arrow[dll, "\lvert \mathrm{Sd}\,h \rvert"] \arrow[dd, "\lvert \beta^{-1}h \rvert"] \\
& \lvert \mathrm{Sd}\,\mathrm{Ex}\,L \rvert \arrow[dl, "\lvert d\mathrm{Ex}\,L \rvert"] \arrow[drr, "\lvert \mu L \rvert"] & \lvert \mathrm{Sd}\,L \rvert \arrow[l, "\lvert \mathrm{Sd}\,eL \rvert"'] \arrow[dr, "\lvert dL \rvert"] & \\
\lvert \mathrm{Ex}\,L \rvert & & & \lvert L \rvert \arrow[lll, "\lvert eL \rvert"']
\end{tikzcd}$$

In view of the naturality of d commutativity holds in the upper left triangle and the trapezium and because of the naturality of β and the fact that (Lemma (7.2)) $dL = \beta^{-1}(eL)$, commutativity also holds in both triangles which have $\lvert \mu L \rvert$ as lower edge. It follows from Lemma (7.4) and (7.5) that the maps $\lvert dL \rvert$, $\lvert eL \rvert$ and $\lvert d\,\mathrm{Ex}\,L \rvert$ are homotopy equivalences. The commutativity in the trapezium and the smallest triangle involving $\lvert \mu L \rvert$

therefore implies that the maps $|Sd\,eL|$ and $|\mu L|$ are also homotopy equivalences. Consequently the lower triangle is commutative up to homotopy and

$$|h| \circ |dK| = |d\mathrm{Ex}\,L| \circ |\mathrm{Sd}\,h| \simeq |eL| \circ |\mu L| \circ |\mathrm{Sd}\,h| \simeq |eL| \circ |\beta^{-1}h|.$$

THE WEIZMANN INSTITUTE OF SCIENCE, REHOVOTH, ISRAEL
COLUMBIA UNIVERSITY, NEW YORK, N. Y.

REFERENCES.

[1] S. Eilenberg and S. MacLane, "Acyclic models," *American Journal of Mathematics*, vol. 75 (1953), pp. 189-199.

[2] S. Eilenberg and J. A. Zilber, "Semi-simplicial complexes and singular homology," *Annals of Mathematics*, vol. 51 (1950), pp. 499-513.

[3] D. M. Kan, "Abstract homotopy I," *Proceedings of the National Academy of Sciences*, vol. 41 (1955), pp. 1092-1096.

[4] ———, "Abstract homotopy II," *ibid.*, vol. 42 (1956), pp. 225-228.

[5] ———, "Abstract homotopy III," *ibid.*, vol. 42 (1956), pp. 419-421.

[6] ———, "Adjoint functors," *Transactions of the American Mathematical Society*, (to appear).

[7] ———, "Functors involving c. s. s. complexes," *Transactions of the American Mathematical Society*, (to appear).

[8] J. W. Milnor, "The geometric realization of a semi-simplicial complex," *Annals of Mathematics*, vol. 65 (1957), pp. 357-362.

[9] J. C. Moore, "Semi-simplicial complexes and Postnikov systems," *Proceedings International Symposium on Algebraic Topology and its Applications* (1956), Mexico.

[10] J. H. C. Whitehead, "Combinatorial homotopy I," *Bulletin of the American Mathematical Society*, vol. 55 (1949), pp. 213-245.

TOPOLOGICAL ABELIAN GROUPS.*[1]

By Fred B. Wright.

1. Introduction.

The principal purpose of this note is to establish the existence, in any topological abelian group, of a closed subgroup which has special importance for the structure theory of the group. This subgroup possesses characteristics which are analogous to those of the radical of a ring. It is perhaps appropriate to call this subgroup the radical of the group.

The radical is a well-known subgroup in certain cases. For example, in a discrete abelian group the radical is the torsion subgroup. More generally, in any locally compact abelian group the radical is the union of all compact subgroups. For the additive group of a real linear topological space E, the radical is the set of all elements of E which are annihilated by any continuous linear functional on E.

It is possible to employ the concept of the radical to furnish novel proofs of some theorems which are usually proved by quite different methods. In particular, it is interesting to observe just how much of the structure theory for locally compact abelian groups can be obtained by such methods. In the final section of this paper, it is shown that almost all of this theory can be established intrinsically. That is to say, most of the structure theory can be developed without the use of such "external" constructions as the character group, the L_1-algebra, or the L_2-space of the group.

2. Preliminary considerations.

Since this paper will be concerned only with abelian groups, it is convenient to use an additive notation for the group operation. In a topological group, it will always be assumed that addition is jointly continuous, that inversion is continuous, and that the Hausdorff separation axiom is satisfied. With some care, the preliminary theory can be developed under weaker restrictions. (A subsequent note will deal with an extension to non-abelian groups.)

This is a convenient place to establish some conventions of notation which will be observed throughout this paper. Let G be a topological abelian group,

---

* Received February 27, 1956; revised January 7, 1957.

[1] Written with the support of the National Foundation grant to Tulane University. The advice and criticism of Professors Goto, Mostert, Pettis and Wallace have contributed much to the present form of this paper.

and let A be any subset of G. Then $\bar{A}$ denotes the closure of A, A^0 denotes the interior of A, and $-A$ denotes the set $\{-a: a \in A\}$. A set A is said to be symmetric if $A = -A$. If k is any positive integer, the set kA is defined to be the set $\{a_1 + \cdots + a_k: a_i \in A\}$, and $(-k)A = k(-A)$. The complement of A is denoted by $\sim A$, so that $\sim A = \{x \in G: x \notin A\}$. The symbol $\square$ denotes the empty subset of G.

If B is another subset of G, then $A \cup B$ and $A \cap B$ denote, respectively, the set-theoretic union and intersection of A and B. The set $\{a + b: a \in A, b \in B\}$ is denoted by $A + B$. The set A is a neighborhood of $B \neq \square$ if $B \subset A^0$.

For $x \in G$, the symbol x denotes ambiguously the element x and the set consisting of the single element x. In particular, 0 denotes either the identity element of G or the subgroup consisting of this element only.

A topological isomorphism between two topological groups is an isomorphism between the groups which is also a homeomorphism. Two groups G, H are said to be topologically isomorphic if there is a topological isomorphism between them, and this is denoted by $G \cong H$. The group G is said to be continuously isomorphic to the group H if there is an isomorphism of G onto H which is continuous.

If G and H are two topological abelian groups, their direct sum $G \oplus H$ is the algebraic direct sum endowed with the cartesian product topology.

DEFINITION 2.1. *If A is any nonvoid subset of a topological abelian group G, let* $s(A) = \{x \in G: x + A \subset A\}$.

Since $s(A)$ always contains 0, $s(A)$ is nonvoid.

DEFINITION 2.2. *A nonvoid subset S of a topological abelian group G is said to be a semigroup in G if* $S \subset s(S)$.

It is clear that S is a semigroup if and only if $2S \subset S$, which is in accord with the usual definition. It is obvious that for any nonvoid set A the set $s(A)$ is a semigroup in G.

DEFINITION 2.3. *A subset A of a topological abelian group G is said to be a regular open set if A is the interior of its closure; that is, if* $A = (\bar{A})^0$. *A subset A of G is said to be an angular*[2] *subset of G if A is open and if* $0 \in \bar{A}$.

If S is a semigroup in G, then $\bar{S}$ is also a semigroup in G, and if $S^0 \neq \square$, then S^0 is also a semigroup in G. If a family of semigroups has a nonvoid intersection, that intersection is a semigroup. The union of a chain of semigroups is a semigroup. A subset A of G is open (closed, regular, angular) if and only if $-A$ is open (closed, regular, angular); A is a semigroup if and only if $-A$ is a semigroup.

---

[2] This terminology is due to Hille [4: Definition 7.6.1].

A necessary and sufficient condition that a subset A of G be a subgroup of G is that A be a symmetric semigroup. Another important class of semigroups are those which are completely asymmetric.

DEFINITION 2.4. *A semigroup S in a topological abelian group G is said to be 0-proper if S does not contain the identity element 0 of G.*

Clearly, S is a 0-proper semigroup in G if and only if $S \cap -S = \square$. If S is not 0-proper, then the set $H = S \cap -S$ is a subgroup of G, and is obviously the largest subgroup of G which is contained in S. Then S is a union of cosets of H. If 0 is an interior point of the semigroup S, then $H = S \cap -S$ is an open subgroup of G, so that S is an open set. It follows that in a connected abelian group G an open semigroup is a 0-proper semigroup in G if and only if it is a proper subset of G.

Semigroups of the form $s(A)$, where A is a nonvoid subset of G, have useful properties. It will be observed that $s(-A) = -s(A)$. Then the set $s(A) \cap s(-A)$ is a symmetric semigroup, and hence a subgroup, in G.

DEFINITION 2.5. *For any nonvoid subset A of G, define $b(A)$ to be the subset $s(A) \cap s(-A)$.*

LEMMA 2.1. *For any nonvoid subset A of G, if $x \in b(A)$ then $x + A = A$.*

Proof. If $x \in b(A)$, then $x + A \subset A$ and $-x + A \subset A$. Thus $x + A \subset A \subset x + A$, and hence $A = x + A$.

THOREM 2.2. *If A is a nonvoid regular open set, then $s(\bar{A}) = s(A)$, $s(A)$ is closed, and therefore $b(A)$ is a closed subgroup of G.*

Proof. By definition, $s(\bar{A}) = \cap \{(\bar{A} - x) : x \in \bar{A}\}$, and hence $s(\bar{A})$ is closed. Furthermore, $s(A) \subset s(\bar{A})$, by the continuity of addition. On the other hand, if $x \in s(\bar{A})$, then $x + \bar{A} \subset \bar{A}$, so that $(x + \bar{A})^0 \subset (\bar{A})^0$. Since A is a regular open set, it follows that $x + A \subset A$. Thus $s(\bar{A}) \subset s(A)$, and the proof is complete.

COROLLARY.[3] *If S is a regular open semigroup in G, then $\bar{S} + \bar{S} \subset \bar{S}$.*

---

[3] Compare with [4: Theorem 7.6.3].

LEMMA 2.3. *If S is an angular semigroup in G, then S is a regular open set.*

This is proved in [4: Theorem 7.6.2]. The existence of angular semigroups is sometimes implied by other hypotheses. For example, see [4: Theorem 7.7.1.]

The results of this section are valid for non-commutative groups, provided $s(A)$ is defined to be $\{x \in G: (x+A) \cup (A+x) \subset A\}$.

3. Maximal 0-proper open semigroups.

Suppose G is a topological abelian group which contains 0-proper open semigroups. Then Zorn's lemma furnishes semigroups which are maximal with respect to these properties. This section is devoted to the properties of maximal 0-proper open semigroups. The problem of existence is deferred to later sections, and the presence or absence of such semigroups has a direct bearing on the structure of a group.

It will be observed that M is a maximal 0-proper open semigroup in G if and only if $-M$ is such a semigroup.

THEOREM 3.1. *If M is a maximal 0-proper open semigroup in a topological abelian group, then M is a regular open set.*

Proof. If $0 \in \bar{M}$, then M is angular, and hence regular, by Lemma 2.3. Otherwise $\bar{M}$ is a 0-proper semigroup, and hence $(\bar{M})^0$ is an open 0-proper semigroup containing M. Since M is maximal, $M = (\bar{M})^0$.

LEMMA 3.2. *Let M be a maximal 0-proper open semigroup in a topological abelian group G, and let n be any positive integer. If x is such that $nx \in M$, then $x \in M$.*

Proof. Define a function f on G by $f(x) = nx$; then f is continuous. If $N = f^{-1}M$, then N is obviously a 0-proper open semigroup containing M. Hence $M = f^{-1}M$.

THEOREM 3.3. *If M is a maximal 0-proper open semigroup in G, then the set $\sim(M \cup -M)$ is identical with the closed subgroup $b(M)$.*

Proof. Set $B = \sim(M \cup -M)$. Since $s(M) \cap -M = \square$, then $s(M) \subset B \cup M$. Since M is a semigroup, then $M \subset s(M)$. If $x \in B$, then the set $W = \bigcup_{k=0}^{\infty} (kx + M)$ is an open semigroup containing M. If $0 \in W$, then there is a positive integer n such that $-nx \in M$, and by Lemma 3.2, it follows that $-x \in M$. This contradicts the choice of $x \in B$. Thus $0 \notin W$, and hence $W = M$. In particular, $x + M \subset M$, so that $x \in s(M)$. Thus $B \subset s(M)$, and therefore $M \cup B = s(M)$. Applying this result to $-M$, it follows that $-M \cup B = s(-M)$. Thus $B = s(M) \cap s(-M)$.

This result shows that G can be written as the disjoint union $G = M \cup b(M) \cup -M$, where M and $-M$ are maximal 0-proper open semigroups in G and $b(M)$ is a closed subgroup of G. This fact plays a vital role in all that follows.

The following three results are useful, and are immediate. Their proofs offer no difficulty.

THEOREM 3.4. *If M is a maximal 0-proper open semigroup in G, then $G = M - M$; that is, G is generated by M.*

The last two theorems in this section complete the circle of ideas centering around the notions of maximality, angularity, and regularity of semigroups, and should be compared with Theorem 3.1.

THEOREM 3.5. *Let M be a maximal 0-proper open semigroup in G. Then the following three statements are equivalent:* (1) *M is not angular,* (2) *M is closed,* (3) *$b(M)$ is open.*

THEOREM 3.6. *Let M be a maximal 0-proper open semigroup in G. Then the following are equivalent statements:* (1) *M is angular,* (2) *$\bar{M} = M \cup b(M)$,* (3) *$b(M)$ is the topological boundary of M.*

The repeated use of subgroups of the form $b(M)$ in the sequel makes it advisable to have a convenient name for them. Theorem 3.3 suggests the following.

DEFINITION 3.1. *A closed subgroup B of a topological abelian group G will be called a residual subgroup of G if there exists a maximal 0-proper open semigroup M of G such that $B = b(M)$; in this case, B is called the residual subgroup belonging to M.*

Every residual subgroup belongs to at least two maximal 0-proper open semigroups in G, and may belong to more.

4. The radical of a topological abelian group. It is now time to introduce the principal definition of this paper.

DEFINITION 4.1. *Let G be any topological abelian group. Denote by T the intersection of all the residual subgroups of G, with the convention that $T = G$ if there are no residual subgroups. The closed subgroup T is* *called the radical of G. If $G = T$, G is said to be a radical group, while if $T = 0$, G is said to be a radical-free group.*[4]

THEOREM 4.1. *If G is a discrete abelian group, then the radical T of G is the torsion subgroup of G.*

Proof. For each $x \in G$, the set $\{kx \colon k \geqq 1\}$ is an open semigroup in G. By definition, $x \in T$ if and only if every open semigroup containing x also contains 0. Thus $x \in T$ if and only if x has finite order.

Clearly the radical will always contain the torsion subgroup. It need not, however, be the closure of the torsion subgroup.

A topological abelian group G is a radical group if and only if there are no 0-proper open semigroups. It follows at once that if G is a radical group and if H is a closed subgroup of G, then G/H is a radical group. Thus, if G is a radical group and if S is an open semigroup in G, then $S \cap -S$ is an open subgroup H of G (Section 2). Then G/H is a discrete radical group, and by Theorem 4.1, is a torsion group. Then the image of S in G/H is in fact a group, and, again by Section 2, S is itself a group. This establishes

THEOREM 4.2. *A topological abelian group G is a radical group if and only if every open semigroup in G is an open subgroup of G.*

A non-discrete example of a radical group is therefore furnished by any compact abelian group [15]. Since there are compact groups with no non-zero elements of finite order, this shows that the radical need not be the closure of the torsion subgroup.

If G is a topological abelian group, any subgroup H of G is a topological group in its induced (subspace) topology. Hence H has its own radical, which may be denoted by T_H. It is obvious that $T_H \subset T \cap H$, where T is the radical of G. Whether or not equality holds in general is an open question, except in special cases. It will be seen below that equality of these two groups does hold for locally compact abelian groups.

DEFINITION 4.2. *Let G be a topological abelian group, and let H be any subgroup of G. Then H is said to be a radical subgroup of G if H is a radical group when H is considered to be a topological group in its induced topology.*

Then H is a radical subgroup of G if and only if $H = T_H$. In such a case, $H \subset T$.

---

[4] Although the terminology "radical" should cause no confusion, it seems advisable to use "radical-free" instead of "semisimple."

LEMMA 4.3. *Let G be a topological abelian group.* (1) *If H is a radical subgroup of G, then $\bar{H}$ is a radical subgroup of G.* (2) *The set-theoretic union of a chain of radical subgroups is a radical subgroup of G.* (3) *The subgroup generated by two radical subgroups of G is also a radical subgroup of G.*

Proof. The proof of (3), for example, will illustrate the proofs of the others. Let H_1 and H_2 be two radical subgroups of G, and let $H = H_1 + H_2$. If M is a maximal 0-proper (relatively) open semigroup in H, then $M \cap H_1 = M \cap H_2 = \square$, and hence both H_1 and H_2 are contained in $b_H(M)$, the residual subgroup in H belonging to M. Thus $H \subset b_H(M)$, and hence no such M can exist.

This yields at once the following result.

THEOREM 4.4. *If G is any topological abelian group, then there exists in G a unique maximal radical subgroup H which is closed and is contained in the radical T of G.*

The question naturally arises: is the radical itself a radical subgroup? In general, this is an open question. For locally compact groups, the answer is affirmative. Another affirmative answer is provided by the next theorem.

THEOREM 4.5. *Let G be a topological abelian group with radical T. If $T \neq G$, the following are equivalent.* (1) *There exists a residual subgroup of G which is open.* (2) *Every residual subgroup of G is open.* (3) *The radical T of G is open. If any one of these is true then the radical T is the unique residual subgroup of G, and T is a radical subgroup of G.*

Proof. It is clear that (3) implies (2) and that (2) implies (1). Finally, assume the residual subgroup $b(M)$ is open, and let S be a 0-proper open semigroup in $b(M)$. Since $b(M) + M = M$, it follows that $S \cup M$ is a 0-proper open semigroup in G, violating the maximality of M. Hence $b(M)$ is a radical group, and hence $b(M) \subset T$, by Theorem 4.4. Since $T \subset b(M)$ in every case, then $T = b(M)$ in this case. This also establishes the last statement of the theorem.

Direct calculation establishes the following behavior of 0-proper open semigroups under certain homomorphisms.

LEMMA 4.6. *Let G be a topological abelian group with radical T, and let H be a closed subgroup of G, such that $H \subset T$. Let G^* denote the quotient group G/H, and let π denote the natural homomorphism of G onto G^*. If M and M^* are 0-proper open semigroups in G and G^* respec-*

tively, then πM *and* $\pi^{-1}M^*$ *are* 0*-proper open semigroups in* G^* *and* G *respectively. If* M *and* M^* *are maximal, then* πM *and* $\pi^{-1}M^*$ *are maximal. In particular, if* M *is a maximal* 0*-proper open semigroup in* G, *then* $M = \pi^{-1}\pi M$.

An immediate corollary of this result is the following useful fact.

THEOREM 4.7. *If* G *is a topological abelian group with radical* T, *and if* H *is a closed subgroup of* G *such that* $H \subset T$, *then the radical of* G/H *is* T/H. *In particular,* G/T *is radical-free.*

The next result characterizes the radical as the minimal subgroup of G satisfying the last statement of the preceding theorem.

THEOREM 4.8. *Let* G *be a topological abelian group with radical* T. *Let* H *be any closed subgroup of* G *such that* G/H *is radical-free. Then* $T \subset H$.

Proof. Let $G^* = G/H$, and let $\pi\colon G \to G^*$ be the canonical homomorphism. If M^* is a maximal 0-proper open semigroup in G^*, then there is a maximal 0-proper open semigroup M in G such that $\pi^{-1}M^* \subset M$. Then $\pi^{-1}b(M^*) \supset b(M)$, where the calculations of residual subgroups are made in the proper groups. Then $\bigcap \pi b(M) \subset \bigcap b(M^*)$, where the right-hand intersection is taken over *all* residual subgroups in G^* and the left-hand intersection is taken over *some* residual subgroups in G. The same inclusion is valid if the left-hand intersection is taken over all residual subgroups of G, obviously. Hence

$$T = \bigcap b(M) \subset \bigcap \pi^{-1}\pi b(M) = \pi^{-1} \bigcap \pi b(M) \subset \pi^{-1} \bigcap b(M^*) = \pi^{-1}0 = H,$$

since G^* is radical-free.

The following manifestly true remarks will be employed from time to time. (1) Any subgroup of a radical-free group is radical-free. (2) A radical-free group remains radical-free if the topology is strengthened. (3) A radical group remains a radical group if the topology is weakened. The last two statements are most useful when translated into terms of continous isomorphisms, and (3) is in fact a special case of a remark following Theorem 4.1 above.

5. Maximally radical-free groups. Certain radical-free groups are of special interest because of their significance in structure theory.

DEFINITION 5.1. *A topological abelian group G is said to be maximally radical-free if the subgroup 0 is a residual subgroup of G.*

Thus G is maximally radical-free if and only if there exists a maximal 0-proper open semigroup M in G with $b(M)=0$. The class of such groups coincides precisely with the class of linearly ordered abelian groups. For, let A be an abelian group (no topology!) which is linearly ordered by the relation $\geqq$. Let P denote the set of all elements x in A satisfying $x>0$. Then P is a 0-proper semigroup in A, and every element of A different from 0 is either in P or in $-P$. If, conversely, P is a 0-proper semigroup in G such that $\sim(P\cup -P)=0$, then there is a linear order in A such that $P=\{x\in A: x>0\}$. The set P is called the positive cone of A.

A linearly ordered abelian group A has an intrinsic topology defined on it by the order. A base for the neighborhoods of 0 is given by the family of intervals $(-a,a)=\{x\in A: -a<x<a\}$, for all $a\in P$. This topology will be called the interval topology in A. It is easily seen that A is a topological abelian group in the interval topology, and that the positive cone P of A is open.

The interval topology is thus essentially determined by the positive cone P. One minor relation between the algebraic structure of P and the topology in A is worth recording. It is easily seen that either $P=2P$ or else $P\cap\sim(2P)$ consists of a single element. In the latter case, the group A is discrete in the interval topology, while if $P=2P$ the group A is dense-in-itself.

Further details about linearly ordered abelian groups may be found in [1]. The remarks above form the skeleton of the very important result contained in the following theorem.

THEOREM 5.1. *Let G be a maximally radical-free topological abelian group. Then G can be made a linearly ordered abelian group, and the interval topology on G is coarser than the original topology. Conversely, if A is a linearly ordered abelian group, then A is a maximally radical-free group in its interval topology.*

This yields an interesting new proof of a classic theorem concerning abelian groups: Any abelian group, all of whose elements have infinite order, can be linearly ordered to be a linearly ordered group [8]. For, if the group is given the discrete topology, it is therefore radical-free (Theorem 4.1). Since the radical is open, it is the unique residual subgroup in the group (Theorem 4.5). Hence the group is maximally radical-free (Definition 5.1).

Thus the group can be made a linearly ordered group (Theorem 5.1). It is interesting to uncover the almost completely hidden use of the axiom of choice, which is usually cited explicitly in proofs of this theorem.

THEOREM 5.2. *A connected maximally radical-free topological abelian group is continuously isomorphic to the additive group of real numbers. If the group is either locally compact or locally connected, then the isomorphism is also a homeomorphism.*

Proof. Such a group has the property that the space obtained by deleting the element 0 is disconnected, by virtue of Theorem 3.3. The conclusion of the theorem follows from [2: page 16, no. 4]. (See also [5] for a precise statement of the theorem cited.)

COROLLARY 1. *Let G be a maximally radical-free group, and let K be the component of* 0 *in G. Then either $K=0$ or K is continuously isomorphic to the additive group of real numbers.*

In the structure theorems which follow, it will be necessary to establish the fact that a continuous isomorphism is in fact a topological isomorphism. This will be done by citing an appropriate one of the following three references: [14: page 20], [14: page 95], [10: Theorem 6]. The first such structure theorem, which follows from the second of these references, is now at hand.

COROLLARY 2. *Let G be a maximally radical-free group, with K the component of* 0 *in G. If G/K is discrete, then G is topologically isomorphic to $K \oplus (G/K)$.*

Now let G be maximally radical-free and let K be the component of 0 in G. Then K has the property that for any $x \in K$, with $x > 0$, if $0 < y < x$ then $y \in K$; that is, K is an "isolated subgroup" [12] or a "convex subgroup" [1] of G. To see this, let H be the set of all elements $y \in G$ such that $-x < y < x$ for all $x > 0$ in K. It is easily seen that $H + K$ is the smallest convex subgroup containing K. But if $y \in M$ is different from 0, the interval $(-y, y)$ is an open set in G containing 0. But $(-y, y) \cap K$ is a neighborhod of 0 in K, and $(-y, y) \cap K = 0$. Hence either $K = 0$ or $H = 0$. In either case K is a convex subgroup, as desired.

Since this is true, the quotient group G/K has an induced linear order [12: Chapter 1, Lemma 2]. Then G/K is maximally radical-free in the interval topology given by this order. It is easy to see that the quotient topology on G/K, where G is considered in its original topology, is finer than the interval topology on G/K. This yields the following result.

THEOREM 5.3. *If G is a maximally radical-free topological abelian group, and if K is the component of 0 in G, then either $G = K$ or else the quotient group G/K is maximally radical-free.*

Maximally radical-free groups occur in structure theory in the form of certain quotient groups.

THEOREM 5.4. *If G is a topological abelian group and if $b(M)$ is a residual subgroup of G, then $G/b(M)$ is maximally radical-free.*

6. Real linear topological spaces.

This section is something of a digression from the prinicipal theme of this paper. It is interpolated here for two reasons. In the first place, the additive group of an infinite dimensional real linear topological space is the most accessible example of a topological abelian group which is not locally compact, but which has almost any other pleasant algebraic or topological property. It is therefore of some interest to see what the radical is for such a group. Of perhaps equal interest is the fact that real linear topological spaces are the natural vehicles for representations of certain abelian groups, as is shown in the next section.

LEMMA 6.1. *Let E be a real linear topological space, and let M be a maximal 0-proper open semigroup in E. Then M is convex.*

Proof. Since M is open, it suffices to show that M is midpoint-convex. Since M is a semigroup, this will follow if it is shown that $x \in M$ implies that $\frac{1}{2}x \in M$. But this follows at once from Lemma 3.2.

This result is sufficient to establish the precise description of a maximal 0-proper open semigroup and its residual subgroup; one needs only to appeal to [7: Theorem 8.10] to obtain the answer.

THEOREM 6.2. *If M is a maximal 0-proper open semigroup in a real linear topological space E, then there exists a continuous linear functional f on E such that $M = \{x \in E : f(x) > 0\}$, $-M = \{x \in E : f(x) < 0\}$, and $b(M) = \{x \in E : f(x) = 0\}$.*

COROLLARY 1. *The set of residual subgroups of a real linear topological space E is in one-to-one correspondence with the set of continuous hyperplanes through 0 in E. The radical of E consists of all those elements of E which are annihilated by every continuous linear functional on E.*

COROLLARY 2.[5] *In any real linear topological space E, if S is an open semigroup in E, then either $S = E$ or S is a subset of a half-space of E.*

It should be noted that the proof of Lemma 6.1 does not depend on either the joint continuity of addition or on the Hausdorff separation axiom. Since [7: Theorem 8.10] also makes no use of these restrictions, this entire section may be extended to such spaces. Theorem 6.2, in particular, shows that the residual subgroups are closed linear subapces. Thus the concept of the radical is applicable to this wider class of linear spaces, and Corollary 1 asserts that a real linear topological space is radical-free if and only if it is a locally convex Hausdorff linear topological space.

7. Representation of connected groups. Throughout this section, let G denote a connected abelian group. If $b(M)$ is a residual subgroup of G, then $G/b(M)$ is continuously isomorphic to the additive group of real numbers. Conversely, if ϕ is a continuous homomorphism of G onto the reals, it is obvious that the kernel $\phi^{-1}0$ of ϕ is the residual subgroup belonging to the pre-image of the open right-half line under ϕ. An easily established necessary and sufficient condition that two continuous homomorphisms ϕ_1 and ϕ_2 of G onto the real line have the same kernel is that there exist a real number α such that $\phi_1(x) = \alpha \cdot \phi_2(x)$ for all $x \in G$.

If E denotes the set of all continuous homomorphisms of G into the real line, then E is a vector space over the reals under pointwise operations. Furthermore, E can be endowed with a topology making it a linear topological space. The most natural, though by no means the only, such topology is the weak topology induced by G. Since G is assumed to be Hausdorff, the space E will also be a Hausdorff space, and it is clearly locally convex in this topology.

Now let E^* denote the dual space of E, and let E^* be given its weak* topology; that is, the topology induced on E^* by E. For each $x \in G$, define $Rx \in E^*$ by setting $Rx(\phi) = \phi(x)$, for each $\phi \in E$. It is clear that R is a homomorphism of G into E^*. Furthermore, $Rx = 0$ if and only if $\phi(x) = 0$ for all $\phi \in E$. As shown above, this holds if and only if x belongs to the radical T of G. The continuity of R follows at once from the definition of the topology in E^*.

Finally, if $\phi \in E$ is such that $\phi(x) = 0$ for all $x \in G$, then $\phi = 0$. This shows that the range of R in E^* generates a linear subspace which is dense in E^* in the weak* topology. These results are summarized as follows.

---

[5] Compare with [4: Theorem 7.6.8].

THEOREM 7.1. *Let G be a connected abelian group with radical T. Then there exists a locally convex real linear topological space E with dual space E^*, and a continuous homomorphism R of G into E^* such that the kernel of R is T. The range of R generates a weak* dense linear subspace of E^*.*

This result is a generalization of part of the structure theorem for locally compact abelian groups. Furthermore, if G is a normed linear space, the mapping R is the usual injection of G into its second dual space, and the last statement of Theorem 7.1 is Helley's theorem.

If the hypothesis of connectivity is replaced by an algebraic condition, analogous results can be established. The algebraic condition is a generalization of Archimedean order. This topic will be dealt with in a subsequent note.

8. Locally compact abelian groups. This final section is concerned with the application of the methods and results of the preceding sections to the study of locally compact abelian groups. The structure of such groups is well-known [11, 13, 14]. The purpose of this section is to establish as much of this structure theory as possible by means of topological and algebraic methods alone, and within the group itself. This means that the proofs to follow will make no use of measure-theoretic concepts, and that no external constructions will be used. In particular, the character group will not be used. (In the proofs of Theorems 8.3 and 8.4, the concept of a covering group [3] is used. This violates the promise not to use non-intrinsic objects. The fact is that these two results can be given intrinsic proofs which amount to proving the one fact about covering groups which is needed. It has seemed simpler to make this concession to the demands of brevity.)

It must be noted that the full structure theorem has not as yet yielded to these methods. Theorem 8.5, Theorem 8.7 and the Corollary to Theorem 8.9 constitute that part which can be so proved. The missing result is precisely this: the radical of a locally compact connected abelian group is a topological and algebraic direct summand of the group. (One can easily reduce the problem to the case in which the radical is divisible, in which case the radical is algebraically a direct summand.)

To begin, it will be recalled that a compact group is a radical group [15]. It follows that every compact subgroup of a locally compact abelian group is contained in the radical. Hence a radical-free group contains no compact subgroups other than 0.

LEMMA 8.1. *Let G be a totally disconnected radical-free locally compact abelian group. Then G is discrete.*

Proof. Since G is totally disconnected, there exists a compact open subgroup H. Since G is radical-free, $H = 0$, so that G is discrete.

LEMMA 8.2. *Let G be a radical-free locally compact abelian group. Then there exists a finite set of residual subgroups $b(M_1) \cdots, b(M_n)$ of G such that the subgroup $B = \bigcap_{j=1}^{n} b(M_j)$ is discrete.*

Proof. Let U be a compact neighborhood of 0, and let W be the boundary of U. When W is compact, and $0 \notin W$. Since G is radical-free, the open sets $(M \cup -M)$, for all maximal 0-proper open semigroups M in G, cover the compact set W. If $(M_1 \cup -M_1), \cdots, (M_n \cup -M_n)$ give a covering of W, consider the closed subgroup $B = \bigcap_{j=1}^{n} b(M_j)$. It follows that $B \cap U = B \cap U^0$. If B_K is the component of 0 in B, then $B_K \cap U$ is a nonvoid open and closed subset of B_K. Hence $B_K \cap U = B_K$, and since B_K is radical-free, then $B_K = 0$. Thus B is totally disconnected and therefore, being radical-free itself, it is discrete.

In what follows, the additive group of a real linear topological space is called a vector group, and the linear dimension of the vector space is called the dimension of the vector group.

THEOREM 8.3. *If G is a connected radical-free locally compact abelian group, then G is topologically isomorphic to a vector group of (unique) finite dimension.*

Proof. Choose the least positive integer such that there exists a collection of n residual subgroups $b(M_1), \cdots, b(M_n)$ with discrete intersection B. It is apparent that there is a one-to-one continuous isomorphism of G/B into the direct sum of the groups $G/b(M_i)$, and the minimality of n shows that the mapping is in fact onto this direct sum. Thus G/B is continuously isomorphic to E^n, where E^n is the Euclidean vector group of dimension n. It follows from [9] or [10: Theorem 6] that this mapping is open, and therefore a homeomorphism.

Since G is connected and B is discrete, it follows that G is a covering group for E^n. The uniqueness of the covering group for E^n implies that $B = 0$, and the proof is complete.

Theorem 8.4. *If G is a connected locally compact abelian group, then the radical T of G is connected.*

Proof. Let H be a subgroup of T which is relatively open in T. By Theorem 4.7 the group G/H has the discrete group T/H as its radical. Thus G/H is a covering group of $(G/H)/(T/H) \cong G/T \cong E^n$. Hence $T/H = 0$, and thus $H = T$.

A complete description of radical-free locally compact abelian groups is now at hand.

Theorem 8.5. *Let G be a radical-free locally compact abelian group, and let K be the component of 0 in G. Then K is topologically isomorphic to a Euclidean vector group E^n, G/K is discrete, and G is topologically isomorphic to $(G/K) \oplus K$.*

Proof (in outline). Suppose first that G is maximally radical-free. Then G/K is totally disconnected, and is maximally radical-free (Theorem 5.3). Thus, by Lemma 8.1, G/K is discrete, and therefore $G = K \oplus (G/K)$, by Corollary 2 to Theorem 5.2.

Theorem 4.5 shows that consideration may be restricted to the case in which $G/b(M)$ is not discrete for any residual subgroup $b(M)$ of G. Since $G/b(M)$ is maximally radical-free, then $G/b(M) = E^1 \oplus D$, where D is discrete, for each M. Now choose the least integer n such that there exists a family $b(M_i)$, $i = 1, \cdots, n$, of residual subgroups of G having discrete intersection B. Then G/B is topologically isomorphic to $E^n \oplus \Delta_1$, where Δ_1 is discrete. Let $\pi: G \rightarrow G/B$ be the canonical homomorphism, and let $\Delta = \pi^{-1}\Delta_1$. Then $G/\Delta \cong E^n$, and it is easily seen that $K \cong E^n$. It follows that there is a continuous homomorphism of G onto K leaving K elementwise fixed. By [14: page 20], $G = K \oplus (G/K)$. Then the totally disconnected group G/K must be radical-free (being essentially a subgroup of G), and is therefore discrete.

Corollary. *If G is a totally disconnected locally compact abelian group, then the radical T of G is open.*

In particular, in the totally disconnected case the radical is the unique residual subgroup and also the maximal radical subgroup of G. This comment will be extended to the general case later.

The next result is the crucial lemma in the study of radical groups.

LEMMA 8.6. *Let G be a locally compact abelian group, and let K be the component of* 0 *in G. If K is not compact, then G is not a radical group.*

Proof. Let U be a symmetric open neighborhood of 0 whose closure is compact. Set $U_1 = U$ and define $U_{n+1} = U_n + U$. Then U_n is open and has compact closure. Since K is not compact, neither is G, and therefore $(U_n)^- \neq G$. On the other hand, if $U_n = (U_n)^-$, then U_n is both open and closed, and since it contains 0 it contains K. This, however, implies that K is compact. Hence $U_n \neq (U_n)^-$. The proof can now be completed by copying the proof of Lemma 2, page 153, of [11]. There it is shown that there exists an element d in the boundary of U such that nd is in the boundary of U_n. This being true, it follows that the set $\bigcup_{n=1}^{\infty} (nd + U_n)$ is a 0-proper open semigroup in G.

A more natural way of expressing this result is as follows.

THEOREM 8.7. *If G is a radical locally compact abelian group, then the component of* 0 *in G is compact.*

COROLLARY. *A necessary and sufficient condition that a connected locally compact abelian group be a radical group is that G be compact.*

It is now necessary to prove directly a piece of the structure theorem. In the usual order of things, this follows as an easy consequence of the theorem. The proof given of this result here is a mild adaptation of the standard construction of a one-parameter subgroup in G.

LEMMA 8.8. *Let G be a locally compact abelian group, and let H be a closed subgroup of G such that H is topologically isomorphic to a vector group E^n, and such that G/H is topologically isomorphic to a vector group E^m. Then G is topologically isomorphic to E^{n+m}.*

Proof. These hypotheses imply that G is connected [3: page 36]. The proof is an induction on m. The case $m = 0$ being trivial, suppose $G/H \cong E^1$. For each integer $k \geqq 1$ and for each $x \in G$, the equation $2^k y = x$ has a unique solution y. (That G is algebraically isomorphic to E^{n+m} follows at once from [6: Theorem 2], for example.) Thus the mappings f_k, defined on G for each positive integer k by $f_k(x) = 2^k x$, are continuous isomorphisms of G onto itself. Since G is connected and locally compact, [10: Theorem 6] applies, and hence f_k is open.

Let U be any compact neighborhood of 0 in G, and let $U_k = j_k^{-1}U$. Then each U_k is a compact neighborhood of 0 in G, and $U_k \supset U_{k+1}$ for each k. Then, given any such U and any $x \in G$ such that $x \notin H$, let $2^{-k}x$ denote the unique solution of the equation $2^k y = x$. If X is the set of all $2^{-k}x$, $k = 1, 2, \cdots$, then $X \subset U$, and since U is compact, $\bar{X}$ is compact and is contained in U. Thus the set X has at least one limit point $a \in U$. It will now be shown that necessarily $a = 0$.

If $2^{-k_i}x \rightarrow a$, as $i \rightarrow \infty$, it is obvious that for each i, $2^{k_i}a \in U$. One of three cases can occur: (1) $a = 0$, (2) $a \neq 0$ has finite order, (3) U contains an infinite number of non-zero elements in the cyclic subgroup spanned by a. Case (2) is ruled out at once, since G has no such elements. If (3) holds for a in G, it also holds for the image of a in $G/H \cong E^1$. This contradiction implies that $a \in H$, and hence (3) holds in $H = E^n$. This is also impossible. Therefore $2^{-k}x \rightarrow 0$ and $k \rightarrow \infty$.

A copy of the reals may now be constructed in G. The group generated by X is disjoint from H, and is a continuously isomorphic copy of the dyadic rationals. Then this isomorphism can be extended to a continuous isomorphism of the reals E^1 into G. The isomorphism is necessarily a homeomorphism (onto its image), and it readily follows that $G \cong E^n \oplus E^1 \cong E^{n+1}$. An easy induction establishes the general result.

It is now possible to establish the important fact that the radical of any locally compact abelian group is a radical subgroup.

THEOREM 8.9. *The radical T of a locally compact abelian group G is the maximal radical subgroup of G.*

Proof. If T is not a radical group, then there is a closed subgroup $H \subset T$ such that H is a residual subgroup of T. Then G/H has T/H as its radical. This reduces the problem to showing that the radical cannot be maximally radical-free. A similar reduction enables one to consider separately the possibility that T is either the additive group of reals or is a discrete torsion-free group.

Suppose first that $T \cong E^1$. Then $T \subset K$, where K is the component of 0 in G. Then $G/K \cong (G/T)/(K/T)$. Since K is connected, it follows that $K/T \cong E^n$ for some integer n. By Lemma 8.8, $K \cong E^{n+1}$. But $G/T \cong E^m \oplus \Delta$, for integer m and a discrete group Δ. Then $G/K \cong E^{m-n} \oplus \Delta$. Since G/K is totally disconnected, $m - n = 0$, so that G/K is discrete. Since K is divisible, $G \cong K \oplus (G/K)$. But then G has radical 0, contrary to assumption.

This leaves the possibility that the radical T is a discrete torsion-free group. As before, $G/T \cong E^m \oplus \Delta$. If K is the component of 0, then $K \cap T$ is a closed discrete subgroup of K containing the radical of K. Since the radical of K is connected, K is radical-free, and hence $K \cong E^n$ for some integer $n \geqq 0$. On the other hand, the group $K/(K \cap T)$ is mapped continuously and isomorphically into the component E^m of G/T. Thus $K/(K \cap T)$ contains no elements of finite order. But if $K \cap T \neq 0$, $K/(K \cap T)$ contains a non-trivial torus, and thus has elements of finite order. Hence $K \cap T = 0$.

Let $H = (K + T)^-$. Since $H/T \subset G/T \cong E^m \oplus \Delta$, then $H/T \cong E^k \oplus \Delta_1$, where Δ_1 is discrete and $k \leqq m$. In the projection of H onto H/T, K is mapped continuously and isomorphically into the component E^k of H/T. Since $G/H \cong (G/T)/(H/T)$, it follows that $G/H \cong E^r \oplus Z^s \oplus \Delta_2$, where Z^s denotes a torus of dimension s, where Δ_2 is discrete, and where $r + s = m - k$. But the left-hand side is totally disconnected, so that $r + s = 0$, and hence $m = k$. Thus $H/T \cong E^m \quad \Delta_1$. Let π denote the projection of H onto H/T. Since π is continuous and since $H = (K + T)^-$, then $E^m \oplus \Delta_1 \cong H/T = \pi H = \pi(K + T)^- \subset (\pi(K + T))^- = (\pi K)^- \subset E^m$. Thus $\Delta_1 = 0$ and $H/T \cong E^m$. Then π yields a continuous isomorphism of $K \cong E^n$ onto a dense subset of E^n. By virtue of [2: Chapter VII, § 2, no. 1], K is closed, so that $H/T \cong E^n \cong K$. It follows at once from [14: page 20] that $H \cong K \oplus \Delta_3$, where Δ_3 is discrete and topologically isomorphic to H/K.

Since G/H is discrete, H is open in G, and since H/K is discrete, K is open in H. Hence K is open in G, so that G/K is discrete. By [14: page 95], $G \cong K \oplus \Delta_4$, where $\Delta_4 \cong G/K$. Since $\Delta_4$is discrete, its radical is its torsion subgroup,. which is contained in T. But T is torsion-free, and hence G has radical 0, contrary to assumption. This completes the proof.

COROLLARY. *If G is a connected locally compact abelian group, then the radical T of G is a connected compact subgroup having the property that G/T is topologically isomorphic to a vector group of (unique) finite dimension.*

THEOREM 8.10. *Let G be a locally compact abelian group. Then the following sets in G are identical: (1) the radical T of G, (2) the maximal radical subgroup of G, (3) the set of all elements x in G such that the cyclic subgroup of G generated by x has compact closure.*

Proof. The equality of (1) and (2) was established in Theorem 8.8.

Clearly set (3) is contained in set (1). Conversely, let $x \in T$, and let K be the component of 0 in T. Then K is compact, and the cyclic group (x) has compact closure if $x \in K$. If $x \notin K$, let x^* be the image of x in the radical group $T^* = T/K$. If $\pi\colon T \to T^*$ is the canonical projection, then $\pi(x)^- \subset (\pi x)^- = (x^*)^-$, so that $(x)^- \subset \pi^{-1}(x^*)^-$. If $(x^*)^-$ is known to be compact, then $\pi^{-1}(x^*)^-$ is also compact, since K is compact. This reduces the question to the totally disconnected case.

If T is totally disconnected, let $x \in T$ and let H be a compact open subgroup of T. Then T/H is a discrete radical group, and hence a torsion group. Then there is some positive integer k such that $kx \in H$. Thus $(x) \subset \bigcup_{i=1}^{k} (ix + H)$, and hence $(x)^-$ is compact.

COROLLARY. *If G is a locally compact abelian group with radical T, and if H is a closed subgroup of G, then the radical of H is $H \cap T$.*

It should be remarked that a more natural order of theorems would be to have Theorem 8.10 follow immediately after Theorem 8.5. In this order, Theorem 8.9 could be eliminated, and Theorem 8.7 could be established with considerable ease (modifying the argument for the result on page 97 of [14]). A direct proof of Theorem 8.10 would, however, be quite similar to the proof of Lemma 8.8.

TULANE UNIVERSITY.

REFERENCES.

[1] G. Birkhoff, "Lattice-ordered groups," *Annals of Mathematics*, vol. 43 (1942), pp. 298-331.

[2] N. Bourbaki, *Topologie Générale* (Actualités Scientifiques et Industrielles, No. 1029), Paris, 1947.

[3] C. Chevalley, *Theory of Lie Groups. I.* Princeton, 1946.

[4] E. Hille, *Functional Analysis and Semigroups*, American Mathematical Society Colloquium Publications, vol. 31, New York, 1948.

[5] T. Ganea, *Zur Charakterisierung einparametriger topologischer Gruppen*, Com. Acad. R. P. Române 1 (1951), pp. 731-732 (Math. Rev. 17 (1956), p. 60).

[6] I. Kaplansky, *Infinite Abelian Groups*, University of Michigan Publications in Mathematics, No. 2, Ann Arbor, 1954.

[7] V. L. Klee, " Convex sets in linear spaces," *Duke Mathematical Journal*, vol. 18 (1951), pp. 443-466.

[8] F. Levi, "Arithmetische Gesetze im Gebiete diskreter Gruppen," *Rendiconti del Circolo Matematico di Palermo*, vol. 35 (1913), pp. 225-236.

[9] E. J. McShane, " Images of sets satisfying the condition of Baire," *Annals of Mathematics*, vol. 52 (1950), pp. 293-308.

[10] B. J. Pettis, " On continuity and openness of homomorphism in topological groups," *Annals of Mathematics*, vol. 52 (1950), pp. 293-308.

[11] L. Pontrjagin, *Topological Groups*, Princeton, 1946.

[12] O. F. G. Schilling, *The Theory of Valuations*, Mathematical Surveys, No. 4, New York, 1950.

[13] E. R. van Kampen, " Locally bicompact abelian groups and their character groups," *Annals of Mathematics*, vol. 36 (1935), pp. 448-463.

[14] A. Weil, *L'intégration dans les groupes topologiques et ses applications*, Paris, 1940.

[15] F. B. Wright, " Semigroups in compact groups," *Proceedings of the American Mathematical Society*, vol. 7 (1956), pp. 309-311.

ON CURVES OF MINIMAL LENGTH WITH A CONSTRAINT ON AVERAGE CURVATURE, AND WITH PRESCRIBED INITIAL AND TERMINAL POSITIONS AND TANGENTS.*[1]

By L. E. Dubins.

1. Introduction and summary. Let a particle pursue a continuously differentiable path from an initial point u to a terminal point v. Suppose that its speed is unity and suppose that its velocity vectors at u and v are U and V respectively. We are interested in a path of minimal length for the particle. It is easy to see that there exist u, U, v and V for which no path of minimal length exists. We need some further reasonable restriction. At first, it seems natural to require that the path possess a curvature everywhere, and to prescribe that its radius of curvature be everywhere greater than or equal to a fixed number R. But again there exist (u, U, v, V, R) for which no path of minimal length exists (Proposition 14). The difficulty is that we have imposed too severe a restriction. In order to arrive at the correct restriction to impose, we observe that if X is a curve in real n-dimensional Euclidean space, parameterized by arc length, for which $X''(s)$ exists everywhere, then the curvature, $\| X''(s) \|$, is less than or equal to R^{-1} everywhere, if and only if,

$$\| X'(s_1) - X'(s_2) \| \leqq R^{-1} \, | s_1 - s_2 |, \tag{1}$$

for all s_1 and s_2 in the interval of definition of X. By the *average curvature* of X in the interval $[s_1, s_2]$ we mean the left side of (1) divided by $| s_1 - s_2 |$. We say that a curve X in real Euclidean n-space parameterized by arc length has *average curvature always less than or equal to* R^{-1} provided that its first derivative X' exists everywhere and satisfies the Lipschitz condition (1). We inquire, for fixed vectors u, U, v, V in real n-dimensional Euclidean space, E_n, and a fixed positive number R, as to the existence and nature of a path of minimal length among the curves in E_n, of average curvature everywhere less than or equal to R^{-1}. Now we find that paths of minimal length necessarily exist. We call such a path an *R-geodesic.* The purpose of this paper

---

* Received April 28, 1956; revised January 3, 1957.

[1] This research was supported in part by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command.

is to prove Theorem 1, which implies that for $n=2$, an R-geodesic is necessarily a continuously differentiable curve which consists of not more than three pieces, each of which is either a straight line segment or an arc of a circle of radius R. Furthermore, the corollary to Theorem 1 implies that three is the least integer for which this is true. The nature of R-geodesics for $n \geqq 3$ is open.

2. Existence of *R*-geodesics. Let u, v, U and V be vectors in real n-dimensional Euclidean space, E_n. Let $\| U \| = \| V \| = 1$ and let $R > 0$. Let $C = C(n, u, U, v, V, R)$ be the collection of all curves X defined on a closed interval $[0, L]$, where $L = L(X)$ varies with X, such that $X(s) \in E_n$ for $0 \leqq s \leqq L$; $\| X'(s) \| = 1$; the average curvature of X is everywhere less than or equal to R^{-1}; $X(0) = u$, $X'(0) = U$, $X(L) = v$ and $X'(L) = V$.

PROPOSITION 1. *For any n, u, U, v, V, and R, there exists an X in $C = C(n, u, U, v, V, R)$ of minimal length.*

Proof. We omit the verification that C is non empty. Let $X_1 \in C$. Let d_1 be the length of X_1 and let d be the infimum of lengths of all curves in C. Clearly $d \leqq d_1$. There exists a sequence $X_n \in C$ such that the length d_n of X_n is monotonely decreasing to d. Since $\| X_n'(s) \| = 1$, it follows that the X_n' are a uniformly bounded family of functions. Since $\| X_n'(s_1) - X_n'(s_2) \| \leqq R^{-1} | s_1 - s_2 |$ for all s_1 and s_2 in the interval $[0, d]$, it follows that the X_n' also form an equicontinuous family on $[0, d]$. Therefore by Ascoli's theorem, [1], there is a subsequence of the X_n whose derivatives converge uniformly on $[0, d]$ to a function Y. For convenience, we assume that X_n is itself such a sequence. It is easy to see that $Y(0) = U$ and $\| Y(s_1) - Y(s_2) \| \leqq R^{-1} | s_1 - s_2 |$ for all s_1 and s_2 in $[0, d]$. Since

$$X_n(s) = X_n(0) + \int_0^s X_n'(t)\,dt = u + \int_0^s X_n'(t)\,dt$$

it follows that for $0 \leqq s \leqq d$,

$$\| X_n(s) - X_m(s) \| \leqq \int_0^s \| X_n'(t) - X_m'(t) \| \,dt \leqq d \cdot \sup \| X_n'(t) - X_m'(t) \|,$$

where the sup is taken over t in $[0, d]$. Therefore X_n converges uniformly in $[0, d]$ to a function X. Since X_n' converges uniformly to Y and X_n converges to X it follows that $X' = (\lim X_n)' = \lim X_n' = Y$. It is elementary to complete the proof of the theorem by showing that $X(d) = v$ and $X'(d) = V$. Namely,

$$\| X(d) - v \| \leqq \| X(d) - X_n(d) \| + \| X_n(d) - v \|$$
$$= \| X(d) - X_n(d) \| + \| X_n(d) - X_n(d_n) \| \leqq \| X(d) - X_n(d) \| + d_n - d$$

which converges to zero as n approaches infinity. Also,

$$\| X'(d) - V \| \leqq \| X'(d) - X_n'(d) \| + \| X_n'(d) - V \|$$
$$= \| X'(d) - X_n'(d) \| + \| X_n'(d) - X_n'(d_n) \| \leqq \| X'(d) - X_n'(d) \|$$
$$+ R^{-1} \,|\, d_n - d \,|$$

which also converges to zero as n approaches ∞. Thus $X(d) = v$, $X'(d) = V$, and therefore $X \in C$, and X is of minimal length.

3. Some preliminary propositions. The purpose of this section is to prove Proposition 6. We begin by borrowing ideas from E. Schmidt's proof, [2], of A. Schur's Lemma and thereby prove:

PROPOSITION 2. *Let X be a curve of average curvature everywhere less than or equal to R^{-1} and Let Z be a semicircle of radius R. Then*

$$\| X'(s) - X'(t) \| \leqq \| Z'(s) - Z'(t) \|, \tag{2}$$

and

$$(X'(s), X'(t)) \geqq (Z'(s), Z'(t)) \tag{3}$$

for all s and t in $[0, \pi R]$. Furthermore, for any fixed s and t, $s < t$, equality holds in (2) if and only if equality holds in (3), and equality holds in (3) if and only if $X(r)$ is an arc of a circle of radius R for $s \leqq r \leqq t$.

Proof. Condition (1) implies that $X''(s)$ exists almost everywhere and is a measurable function of s bounded by R^{-1}. Therefore

$$\left| \int_s^t \| X''(r) \| \, dr \right| \leqq R^{-1} \,|\, s - t \,|.$$

Since X' is absolutely continuous, we see that the arc length of the curve $X'(r)$ for $s \leqq r \leqq t$ is less than or equal to $R^{-1} \,|\, s - t \,|$. Sincs $X'(r)$ is a curve on the surface, S_n, of the unit sphere in E_n, it follows that the length of a geodesic on this surface which connects $X'(s)$ and $X'(t)$ is certainly less than or equal to $R^{-1} \,|\, s - t \,|$. That is, the great circle on S_n containing both $X'(s)$ and $X'(t)$ is divided into two arcs by $X'(s)$ and $X'(t)$. The length of the smaller of these is $\leqq R^{-1} \,|\, s - t \,|$. It is well known that if two great circular arcs on the unit sphere in E_n are each of length less than or equal to π, then the length of the chord subtended by the smaller arc is less than or equal to the length of the chord subtended by the larger arc.

Therefore, for $R^{-1}|s-t| \leqq \pi$, $\|X'(s)-X'(t)\|$ is less than or equal to the length of the chord subtended by a great circular arc of length $R^{-1}|t-s|$. It is easy to see that for $|t-s| \leqq \pi R$, $\|Z'(s)-Z'(t)\|$ is the length of such a chord. Therefore $\|X'(s)-X'(t)\| \leqq \|Z'(s)-Z'(t)\|$ for $|s-t| \leqq R\pi$. This completes the proof of the first part of the proposition.

It is trivial that if $X(r)$ is an arc of a circle of radius R for $s \leqq r \leqq t$, then $\|X'(s)-X'(t)\| = \|Z'(s)-Z'(t)\|$. Assume, therefore, for some s and t, $0 \leqq s < t \leqq \pi R$, that $\|X'(s)-X'(t)\| = \|Z'(s)-Z'(t)\|$. It follows that the length of the smaller great circular arc between $X'(s)$ and $X'(t)$ equals $R^{-1}|s-t|$. Therefore the arc length of the curve X', for $s \leqq r \leqq t$, is $\geqq R^{-1}|s-t|$. Since it was previously shown to be $\leqq R^{-1}|s-t|$, we conclude that it equals $R^{-1}|s-t|$. Therefore X' is a geodesic on S_n connecting $X'(s)$ with $X'(t)$. Therefore $X'(r)$ is an arc of a unit circle of length $R^{-1}|s-t|$ for $s \leqq r \leqq t$. It now easily follows that $X(r)$ is an arc of a circle of radius R for $s \leqq r \leqq t$. The remainder of the proof of the proposition is trivial.

PROPOSITION 3. *Let X be a curve of average curvature everywhere less than or equal to R^{-1} and let Z be a semicircle of radius R. Let γ be the vector of length R determined by the condition that $Z(0)+\gamma$ is the center of the semicircle Z. Let λ be any vector of length R orthogonal to $X'(0)$. Then*

$$(Z'(s),\gamma) \geqq (X'(s),\lambda) \tag{1}$$

for $0 \leqq s \leqq \frac{1}{2}\pi R$. Furthermore equality holds for some s in this interval if and only if $X(r)$ is an arc of a circle of radius R for $0 \leqq r \leqq s$, and λ is the vector of length R determined by the condition that $X(0)+\lambda$ is the center of the circle determined by X.

Proof. It is easy to see that $Z'(s)$ is a linear combination of the two unit orthogonal vectors $Z'(0)$ and γ/R. Therefore

$$1 = (Z'(s),Z'(s)) = (Z'(s),Z'(0))^2 + (Z'(s),\gamma/R)^2. \tag{2}$$

By Proposition 2, we have,

$$(X'(s),X'(0)) \geqq (Z'(s),Z'(0)). \tag{3}$$

Since $(Z'(s),Z'(0)) \geqq 0$ for $0 \leqq s \leqq \frac{1}{2}\pi R$, we see that (3) implies

$$(X'(s),X'(0))^2 \geqq (Z'(s),Z'(0))^2. \tag{4}$$

Combining (2) and (4) we get

$$1 \leqq (X'(s),X'(0))^2 + (Z'(s),\gamma/R)^2. \tag{5}$$

Since λ/R and $X'(0)$ are unit orthogonal vectors, it follows that

$$(6)\qquad 1=(X'(s),X'(s))\geqq(X'(s),X'(0))^2+(X'(s),\lambda/R)^2.$$

From (5) and (6) we immediately obtain

$$(7)\qquad (Z'(s),\gamma/R)^2\geqq(X'(s),\lambda/R)^2.$$

Since $(Z'(s),\gamma/R)\geqq 0$ for $0\leqq s\leqq\frac{1}{2}\pi R$, we conclude from (7) that

$$(8)\qquad (Z'(s),\gamma)\geqq(X'(s),\lambda)$$

for $0\leqq s\leqq\frac{1}{2}\pi R$. This proves the first part of the proposition.

Assume now, for some s, $0\leqq s\leqq\frac{1}{2}\pi R$, that equality holds in (8). It is easy to see that, therefore, equality must hold in (7). This implies that equality must hold in both (5) and (6) for this particular s. From the equality in (5) we obtain equality in (4) and hence, equality in (3). Therefore, by Proposition 2, $X(r)$ is an arc of a circle of radius R for $0\leqq r\leqq s$. Equality in (6) implies that $X'(s)$ is spanned by $X'(0)$ and λ/R. Since λ is orthogonal to $X'(0)$ it is either the vector determined by the condition that $X(0)+\lambda$ is the center of the semicircle X or the negative of this vector. For $0<s\leqq\frac{1}{2}\pi R$, it is not the negative of this vector since $0<(Z'(s),\gamma)=(X'(s),\lambda)$.

PROPOSITION 4. *Let X be a curve with average everywhere less than or equal to R^{-1} and let λ be any vector of length R orthogonal to $X'(0)$. Then*

$$(X(s)-X(0)-\lambda,X'(s))\geqq 0$$

for $0\leqq s\leqq\frac{1}{2}\pi R$. Furthermore, equality holds for some s in this interval if and only if $X(r)$ is an arc of a circle of radius R for $0\leqq r\leqq s$ and λ is the vector of length R determined by the condition that $X(0)+\lambda$ is the center of the circle determined by X.

Proof. It is easy to see that

$$(9)\qquad (X(s)-X(0)-\lambda,X'(s))=\int_0^s(X'(t),X'(s))dt-(\lambda,X'(s)),$$

for

$$(X(s)-X(0)-\lambda,X'(s))=(X(s)-X(0),X'(s))-(\lambda,X'(s))$$

$$(10)\qquad =(\int_0^s X'(t)dt,X'(s))-(\lambda,X'(s))$$

$$=\int_0^s(X'(t),X'(s))dt-(\lambda,X'(s)).$$

Let $Z(s)$ and γ be as in the hypothesis of Proposition 3. Then Propositions 2 and 3 imply that (10) is greater than or equal to

$$\int_0^s (Z'(t), Z'(s))\,dt - (\gamma, Z'(s)). \tag{11}$$

It is easy to see that (11) is equal to

$$(Z(s) - Z(0) - \gamma, Z'(s)) \tag{12}$$

for the argument is the same as the one which established equality in (9). We now observe that (12) equals one half of

$$d(Z(s) - Z(0) - \gamma, Z(s) - Z(0) - \gamma)/ds, \tag{13}$$

which in turn is equal to

$$d \,\| Z(s) - Z(0) - \gamma \|^2/ds = dR^2/ds = 0. \tag{14}$$

We now prove the second part of the theorem. Assume that for some s, $0 < s \leqq \frac{1}{2}\pi R$,

$$(X(s) - X(0) - \lambda, X'(s)) = 0. \tag{15}$$

Thus the inequalities from (9) through (14) become equalities. In particular, (10) equals (11). But in virtue of Propositions 2 and 3, equality in (10) and (11) imply:

$$\int_0^s (X'(t), X'(s))\,dt = \int_0^s (Z'(t), Z'(s))\,dt; \tag{16}$$

and

$$(\lambda, X'(s)) = (\gamma, Z'(s)). \tag{17}$$

Thus if (15) holds, (17) necessarily also holds. We now invoke the second part of Proposition 3 to complete the proof of the non-trivial part of the present theorem.

Our previous propositions are valid for curves X in any Euclidean space. However, our next two propositions deal only with planar curves. At each point of a differentiable planar curve X there are two tangent circles of radius R. The curve X induces on each of these circles an orientation, so that one of these circles is oriented clockwise, the other counterclockwise. *Let Z_s and Y_s be, respectively, the counterclockwise and clockwise oriented circles of radius R, tangent to the curve X at the point $X(s)$.*

PROPOSITION 5. *Let X be a planar curve with average curvature everywhere less than or equal R^{-1}. Let $D(s)$ be the distance between the center* *of the circle* Y_s *and the center of the circle* Z_0. *Then* $D(s)$ *is a monotone non-decreasing function of s for* $0 \leqq s \leqq \frac{1}{2}\pi R$. *Furthermore,* $D(s) = D(0)$ *for some s in this interval if and only if* $X(r)$ *is a continuously differentiable curve in* $[0, s]$ *such that, for some* r_0 *in the closed interval* $[0, s]$, $X(r)$ *is a counterclockwise oriented arc of a circle of radius R for* $0 \leqq r \leqq r_0$ *and* $X(r)$ *is a clockwise oriented arc of a circle of radius R for* $r_0 \leqq r \leqq s$.

Proof. Let $f(s)$ equal $D^2(s)$. We show that f is non-decreasing. Let T be a rotation through an angle of $\frac{1}{2}\pi$ in the counterclockwise direction. Clearly

$$D(s) = \| X(s) - RT(X'(s)) - X(0) - RT(X'(0)) \|. \tag{18}$$

Since both X and X' are absolutely continuous and the product of two absolutely continuous functions is likewise absolutely continuous, it follows that $f(s)$ is absolutely continuous. Furthermore

$$f'(s) = 2(X(s) - RT(X'(s)) - X(0) - RT(X'(0)), X'(s) - RTX''(s)), \tag{19}$$

Since $T(X'(s))$ is orthogonal to both $X'(s)$ and $T(X''(s))$, it follows that

$$f'(s) = 2(X(s) - X(0) - RTX'(0), X'(s) - RTX''(s)) \tag{20}$$

for all s for which $X''(s)$ exists. Furthermore, $-T(X''(s))$ is some scalar multiple of $X'(s)$, say, $-T(X''(s)) = k(s)X'(s)$. Therefore

$$f'(s) = 2(X(s) - X(0) - RTX'(0), X'(s) + Rk(s)X'(s)) \tag{21}$$

or equivalently,

$$f'(s) = (1 + Rk(s))(X(s) - X(0) - RTX'(0), X'(s)) \tag{22}$$

for all s such that $k(s)$ exists. Furthermore, since $\| X''(s) \| \leqq R^{-1}$,

$$1 + Rk(s) \geqq 0. \tag{23}$$

We easily conclude from (22), (23) and Proposition 4 that $f'(s) \geqq 0$ almost everywhere. Since we already showed that $f(s)$ is absolutely continuous it follows that $f(s)$ is montone non-decreasing. Hence, so is $D(s)$.

This completes the proof of the first part of the theorem. Now assume that $D(s) = D(0)$ for some s with $0 < s \leqq \frac{1}{2}\pi R$. Since D is monotone it follows that $D(r) = D(0)$ for all r with $0 \leqq r \leqq s$. Therefore, $f(r) = D^2(r)$ is constant and consequently $f'(r) = 0$ for $0 \leqq r \leqq s$. It follows from (22) that for every r for which $k(r)$ exists, either

(24) $1 + Rk(r) = 0$ or (25) $(X(r) - X(0) - RTX'(0), X'(r)) = 0$.

Let r_0 be the least upper bound of the set of r in $[0, s]$ for which (25) holds. By continuity of X and X', it is easy to show that (25) also holds for $r = r_0$. By the second part of Proposition 4, we conclude that $X(r)$ is an arc of a circle of radius R for $0 \leqq r \leqq r_0$. Again by (25), we conclude that this arc is counterclockwise oriented. Suppose $r_0 < s$. Then for all r in the half-closed interval $(r_0, s]$ for which $k(r)$ exists, (24) holds. Thus $k(r) = -R^{-1}$ for all r in $(r_0, s]$ for which $k(r)$ exists. Since X' is absolutely continuous, it is easy to prove, therefore, that $X(r)$ is an arc of a circle of radius R for $(r_0, s]$. Since $k(r)$ is negative this arc is clockwise oriented. Since X and X' are continuous at $r = r_0$, the proposition is proven.

As an immediate corollary to Proposition 5 we obtain the main result of this section:

PROPOSITION 6. *Let X be a planar curve with average curvature everywhere less than or equal to R^{-1} and let s be any point in the closed interval $[0, \frac{1}{2}R\pi]$. Then the circle Y_s is either disjoint from, or tangent to, the circle Z_0. Furthermore Y_s is tangent to Z_0 if and only if $X(r)$ is a continuously differentiable curve for $0 \leqq r \leqq s$ such that, for some r_0 in the closed interval $[0, s]$, $X(r)$ is a counterclockwise oriented arc of a circle of radius R for $0 \leqq r \leqq r_0$, and $X(r)$ is a clockwise oriented arc of a circle of radius R for $r_0 \leqq r \leqq s$.*

It is of course obvious that there is a proposition similar to Proposition 6 which is concerned with the circles Z_s and Y_0, rather than Z_0 and Y_s. We do not state this theorem but will also refer to it as Proposition 6 in the sequel.

4. Certain curves are *R*-geodesics.

The purpose of this section is to prove Proposition 9 which states that certain curves, composed of arcs of circles of radius R and straight line segments, are R-geodesics.

Let $X(s)$ be a convex arc defined for $a \leqq s \leqq b$. Let m be the line determined by the two points $X(a)$ and $X(b)$ and let T be the perpendicular projection onto the line m. We will say that a *point p is above the curve X* provided the line segment whose end points are p and $T(p)$ contains a point of the arc $X(s)$. And we will say that a *curve $Y(s)$* defined for $c \leqq s \leqq d$ *lies above the curve $X(s)$* provided that the image under T of all point of Y which lie above the curve X is the segment whose end points are $X(a)$ and $X(b)$.

We state without proof the following proposition which is geometrically obvious.

PROPOSITION 7. *Let X and Y be planar curves defined on the intervals*

$[a,b]$ and $[c,d]$ respectively. Suppose that X is a convex arc and that $X(a)=Y(c)$ and $X(b)=Y(d)$. Then if Y lies above X the arc length of Y is not less than the arc length of X, and equality holds if and only if Y is a one-one parameterization of the range of X.

As an immediate corollary we have:

PROPOSITION 8. (See fig. 1.) *Let d be the length of the smaller arc of a circle Z determined by two points A and B on Z. Let m be the half ray perpendicular to Z at B which does not meet the interior of Z. Suppose $Y(s)$ is a continuous curve parameterized by arc length for $0 \leqq s \leqq L$ which has no point in the interior of Z. Suppose that $Y(0)=A$ and $Y(L)$ is on m. Then $L \geqq d$ and equality holds if and only if $Y(s)$ is a* 1-1 *parameterization of the smaller arc AB.*

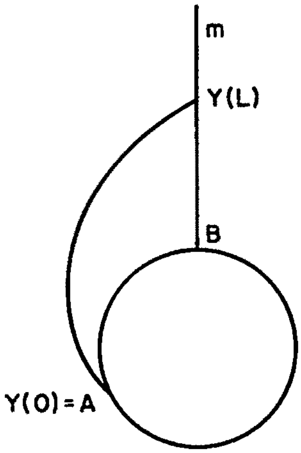

Figure 1.

We will say that a continuously differentiable curve Y, with arc length s as parameter, defined for $a \leqq s \leqq d$, is of *type ALA* (Arc, Line, Arc) provided there exist b and c with $a \leqq b \leqq c \leqq d$ such that Y restricted to $[a,b]$ is a 1-1 parameterization of an arc of a circle of radius R of length less than or equal to $\frac{1}{2}R\pi$, and such that Y restricted to $[b,c]$ is a line segment, and such that Y restricted to $[c,d]$ is also an arc of a circle of radius R of length less than or equal to $\frac{1}{2}R\pi$.

PROPOSITION 9. *Let u, v, U, and V be vectors in Euclidean 2 space with $\| U \| = \| V \| = 1$ and let R be a positive real number. Suppose Y is* *of type ALA defined for* $0 \leqq s \leqq d$, *and suppose* $Y(0) = u$, $Y'(0) = U$, $Y(d) = v$ *and* $Y'(d) = V$. *Then* Y *is the unique R-geodesic in the collection* $C = C(2, u, U, v, V, R)$.

Proof. Suppose that $0 \leqq d_1 \leqq d_1 + d_2 \leqq d$ and that Y restricted to $[0, d_1]$ is an arc of a circle, Z_1, of radius R and length $\leqq \frac{1}{2}R\pi$, and that Y restricted to $[d_1, d_1 + d_2]$ is a line segment, and Y restricted to $[d_1 + d_2, d]$ is an arc of a circle, Z_2, of radius R and length less than or equal to $\frac{1}{2}R\pi$. Let m_1 be the line passing through $Y(d_1)$ and perpendicular to Y at $Y(d_1)$ and let m_2 be the line parallel to m_1 which passes through $Y(d_1 + d_2)$. The plane is divided by m_1 and m_2 into three strips. Now let X be any curve in C. By a connectedness argument, it is easy to see that there is a least positive number s_1 such that $X(s_1)$ is on m_1. We claim $s_1 \geqq d_1$. For either, for all s, $0 \leqq s \leqq s_1$, $X(s)$ is not in the interior of the circle Z_1, or, for some $s_0 < s_1$, $X(s_0)$ is in the interior of Z_1. In the first case, the preceding proposition implies that $s_1 \geqq d_1$. In the second case, Projosition 6 implies that $s_0 > \frac{1}{2}\pi R$. Since $s_1 > s_0 > \frac{1}{2}\pi R \geqq d_1$, it follows that $s_1 > d_1$. Again by a connectedness argument, there is a smallest number s_2 such that $X(s_2)$ is on m_2. Since m_1 and m_2 are a distance d_2 apart, it follows that $s_2 \geqq s_1 + d_2$. Suppose L is any number such that $X(L) = Y(d)$. An argument similar to the one which showed $s_1 \geqq d_1$ will prove that $L - s_2 \geqq d - (d_1 + d_2)$. Therefore $L \geqq d$. Thus we've shown that Y is an R-geodesic in C. Furthermore the conditions for equality in the preceding proposition imply that Y is the unique R-geodesic in C. This completes the proof.

5. Another preliminary proposition. It is the purpose of this section to prove Proposition 13 which states that an R-geodesic consists of pieces, each of which is either a straight line segment or an arc of a circle of radius R. But first we need a few preliminary definitions and propositions.

Let $L(s)$ be a parameterized straight line segment for $a \leqq s \leqq b$, where s is arc length for L. We will say that the line segment *leaves a curve* $X(s)$ *at the point* $X(s_0)$, provided that $L(a) = X(s_0)$ and $L'(a) = X'(s_0)$. Similarly, we say that the parameterized line segment *arrives at the curve* $X(s)$ *at the point* $X(s_0)$, provided that $L(b) = X(s_0)$ and $L'(b) = X'(s_0)$.

We state without proof the following obvious geometric fact.

PROPOSITION 10. *If* $C(s)$ *and* $B(s)$ *are any two distinct similarly oriented parameterized circles of radius* R *in a plane, then there exists a unique parameterized straight line segment which leaves* $C(s)$ *and arrives at* $B(s)$. *Furthermore if* $C(s)$ *and* $B(s)$ *are oppositely oriented then there* *exists a parameterized straight line segment which leaves $C(s)$ and arrives at $B(s)$ if and only if no point of $B(s)$ is in the interior of $C(s)$. If such a segment exists, then it is unique.*

PROPOSITION 11. *Let X be a planar curve with average curvature everywhere less than or equal to R^{-1} defined for $0 \leqq s \leqq d \leqq \pi R/8$. Then the collection $C = C(2, X(0), X'(0), X(d), X'(d), R)$ contains a curve W of type ALA.*

Proof. It is convenient to assume that the plane π which contains the curve X is the collection of all ordered couples of real numbers. It is clearly no loss of generality to assume that $X(0) = (0,0)$ and that $X'(0) = (1,0)$. We consider the four circles Z_0, Z_d, Y_0, Y_d. Clearly Z_0 and Y_0 are the circles of radius R with centers respectively at $(0, R)$ and $(0, -R)$. It is an easy consequence of Proposition 6 that if $X(d)$ is on Y_0 or Z_0, then X is an arc of Y_0 or Z_0 respectively. In this event, X is itself of type *ALA*. Therefore we can assume that $X(d)$ is on neither Z_0 nor Y_0. An application of the techniques of Section 3 shows that the first coordinates of the centers of Z_d and Y_d are strictly positive. There are only three cases to consider: (1) every point on Z_d has a non-negative second coordinate; (2) every point on Y_d has a non-positive second coordinate; (3) some, but not all, points on Z_d have negative second coordinates, and some, but not all, points on Y_d have positive second coordinates. We first consider case (1). Proposition 10 assures the existence of a unique parameterized line segment m which leaves Z_0 and arrives at Z_d. There are now two subcases: (a), the slope of m is less than or equal to the slope of $X'(d)$; and (b), the slope of m is greater than the slope of $X'(d)$. Suppose (a) holds. Let A_1 be the smaller arc of Z_0 whose end points are $(0,0)$ and the point of tangency of m with Z_0. Let A_2 be the smaller arc of Z_d whose end points are $X(d)$ and the point of tangency of m with Z_d. Then one sees that the curve, W, which consists of A_1, followed by m, followed by A_2, satisfies the conclusion of the proposition. Suppose now that subcase (b) holds. Proposition 6 implies that Z_0 and Y_d do not intersect. Therefore Proposition 10 assures the existence of a unique parameterized line segment n which leaves Z_0 and arrives at Y_d. This time we let A_1 be the smaller arc of Z_0 whose end points are $(0,0)$ and the point of tangency of n with Z_0. Similarly, we let A_2 be the smaller arc of Y_d whose end points are $X(d)$ and the point of tangency of n with Y_d. This time one sees that the curve, W, which consists of A_1, followed by n, followed by A_2, satisfies the conclusion of the theorem.

Case (2) is treated similarly. We proceed to case (3). It is clear that the first coordinates of the centers of Z_d and Y_d are unequal. We suppose the first coordinate of the center of Z_d to be less than that of Y_d. The other case can be treated similarly. Propositions 6 and 10 assure the existence of a unique directed line segment m which leaves Y_0 and arrives at Z_d. Let A_1 be the smaller arc of Y_0 whose end points are $(0,0)$ and the point of tangency of m with Y_0. Let A_2 be the smaller arc of Z_d whose end points are $X(d)$ and the point of tangency of m with Z_d. Then one sees that the curve, W, which consists of A_1, followed by m, followed by A_2, satisfies the conclusion of the proposition. This completes the proof.

As an immediate corollary to Propositions 9 and 11 we have:

PROPOSITION 12. *Let X be a planar curve of length less than or equal to $\pi R/8$. Then X is an R-geodesic if and only if X is of type ALA.*

We can now easily establish the main result of this section.

PROPOSITION 13. *Let X be a planar curve defined on a closed finite interval $[0,d]$ parameterized by arc length. Then if X is an R-geodesic, it is a continuously differentiable curve which consists of a finite number of pieces, each of which is either a straight line segment, or an arc of a circle of radius R.*

Proof. Since X' satisfies a Lipschitz condition, X is continuously differentiable. The interval $[0,d]$ can be partitioned into a finite number of subintervals each of length less than or equal to $\pi R/8$. Clearly, X restricted to any of these subintervals is also an R-geodesic. Therefore by the preceding proposition, X, so restricted, is of type ALA. This completes the proof.

6. Principal result.

We wish to show that a planar R-geodesic is necessarily a very special curve, i. e. a continuously differentiable curve which consists of at most *three* pieces, each of which is either a straight line segment or an arc of a circle of radius R. Errett Bishop pointed out to the author that in view of Proposition 13 it is sufficient to show that no curve which consists of four such pieces can be an R-geodesic.

Let us designate a continuously differentiable curve by $CCCC$, provided that it consists of precisely four arcs of circles of radius R. Similarly let us designate by $CLCL$ a continuously differentiable curve which consists of precisely four pieces, the first of which is an arc of a circle of radius R, the second a line segment, the third an arc of a circle of radius R, and the last a line segment. Similarly any differentiable curve which consists of precisely n arcs of circles of radius R and line segments can be represented by an n-tuple of symbols, each of which is either a C or an L.

We already know that there exist planar R-geodesics of type CLC. We will show that there exist planar R-geodesics of type CCC. It is easy to see that any subpath of an R-geodesic is an R-geodesic. We will show that

* *every R-geodesic is necessarily a subpath of a path of type CLC or of type CCC.*

In order to prove that every R-geodesic is necessarily a subpath of a path consisting of three arcs and line segments, it is sufficient to show that no path consisting of four arcs and line segments can be an R-geodesic. There are eight paths of this type, namely $CCCC$, $CCCL$, $CCLC$, $CLCC$, $CLCL$, $LCCC$, $LCCL$ and $LCLC$. If a curve is an R-geodesic, then so is the curve obtained by traversing the path in the opposite direction. Therefore, if we can show that no curve of type $CCLC$ is an R-geodesic, we will also have shown that no curve of type $CLCC$ is an R-geodesic. Thus we wish to show that no curves of type $CCCC$, $CCCL$, $CCLC$, $CLCL$ and $LCCL$, are R-geodesic. Also, if a curve is an R-geodesic, then so is every subpath of the curve. Thus if we can show that no curve of type CCL is an R-geodesic it will follow that neither are curves of type $CCCL$, $CCLC$ and $LCCL$. Likewise, if we can show that no curve of type LCL is an R-geodesic, it will follow that neither is one of type $CLCL$. *Thus in order to show * it is sufficient to show that none of the following three types of curves is an R-geodesic: CCCC, CCL, LCL.* We begin with a proof that no curve of type LCL is an R-geodesic. The proof that no curve of type CCL is an R-geodesic is rather similar, and is therefore omitted. We then show that no curve of type $CCCC$ is an R-geodesic.

LEMMA 1. *If X is a curve of type LCL defined for $0 \leqq s \leqq d$, then it is not an R-geodesic.*

Proof. Let $P_1P_2P_3P_4$ be a curve of type LCL where: (1) P_1P_2 is a line segment, (2) P_2P_3 is an arc of circle of radius R, (3) P_3P_4 is a line segment, (4) P_1P_2 is tangent to P_2P_3 at P_2 and (5) P_3P_4 is tangent to P_2P_3 at P_4.

It is obvious that we may assume P_2P_3 counterclockwise oriented and we do so. We now consider two cases.

Case 1. (See fig. 2.) The length of the arc P_2P_3 is greater than zero but not greater than πR. It is easy to see, by considering subpaths, that we may assume that P_1P_2 and P_3P_4 have the same length. Let S_1 be the counterclockwise oriented circle of radius R, tangent to P_2P_1 at P_1, which is on the same side of P_1P_2 as is the arc P_2P_3. Similarly, let S_2 be the counterclockwise oriented circle of radius R, tangent to P_3P_4 at P_4 which is on the same side of P_3P_4 as is the arc P_2P_3. There exists a unique line segment Q_1Q_2 which leaves S_1 and arrives at S_2. Since the arc length of P_2P_3 does not exceed πR, the curve $P_1Q_1Q_2P_4$ is of type ALA, and hence, by Proposition 9, it is the unique R-geodesic with initial and final positions $X(0)$ *and* $X(d)$ respectively, and initial and final tangent vectors $X'(0)$ and $X'(d)$ respectively.

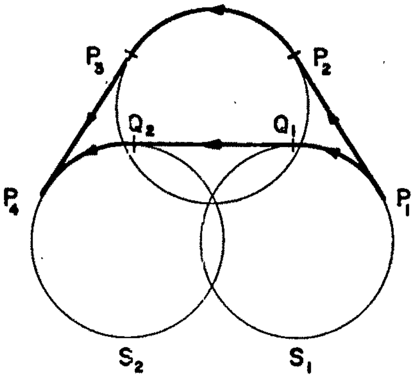

Figure 2.

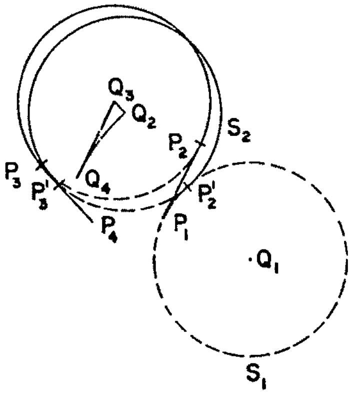

Figure 3.

Case 2. (See fig. 3.) The length of the arc P_2P_3 is strictly between πR and $2\pi R$. It is clear that by considering subpaths we may assume that the segments P_1P_2 and $P_3\ P_4$ do not intersect. Let S_1 *be* the clockwise oriented circle of radius R tangent to P_1P_2 at P_1 which is on the opposite side of P_1P_2 as is the arc P_2P_3. Let S_2 be the counterclockwise oriented circle of radius R which is tangent to S_1 and to P_3P_4. Let P_2' and P_3' be the points of tangency of S_2 with S_1 and P_3P_4 respectively. We will complete our proof by showing that the path $P_1P_2'P_3'P_4$ has length strictly less than the length of X, where: (a) P_1P_2' is the shorter arc of S_1 with end points P_1 and P_2'; and (b) $P_2'P_3'$ is the longer arc of S_2 with end points P_2' and P_3'; and (c) $P_3'P_4$ is the line segment with end points P_3' and P_4. It is sufficient to show that $P_1P_2'P_3'$ is shorter than $P_1P_2P_3P_3'$, where P_1P_2 and P_2P_3 were as defined above and where P_3P_3' is the line segment with end points P_3 and P_3'. There should be no ambiguity in the remainder of this proof if we use the symbol P_2P_3 to represent the length of the arc P_2P_3 as well as the arc itself, similarly for other arcs and line segments. Thus we will complete our proof by showing

$$(1) \qquad P_1P_2' + P_2'P_3' < P_1P_2 + P_2P_3 + P_3P_3'.$$

Let u_2 and u_2' be defined by $Ru_2 = P_2P_3$ and $Ru_2' = P_2'P_3'$. Let u_1' be the angle between the tangent vectors to S_1 at P_1 and P_2'. It is easy to see that (1) is equivalent to

$$(2) \qquad P_1P_2' + Ru_2' < P_1P_2 + Ru_2 + P_3P_3'.$$

Furthermore, since $u_2 = u_2' - u_1'$ we see that (2) is equivalent to

$$(3) \qquad P_1P_2' + Ru_1' < P_1P_2 + P_3P_3'.$$

For $i = 1$ and 2, let Q_i be the center of S_i. P_2P_3 is an arc of a circle whose center we designate by Q_3. Let Q_4Q_2 be the arc of the circle of radius $2R$ with center Q_1, which is concentric with the arc P_1P_2'. Clearly, the arc Q_4Q_2 has a length equal to the left side of (3), whereas the segments Q_4Q_3 and Q_3Q_2 have lengths equal respectively to P_1P_2 and P_3P_3'. Thus (3) is equivalent to

$$(4) \qquad Q_4Q_2 < Q_4Q_3 + Q_3Q_2.$$

Since the arc $Q_4Q_3Q_2$ lies above the convex arc Q_4Q_2, Proposition 7 implies (4). This proves the lemma.

We are indebted to Errett Bishop for the main ideas in the proof of the following lemma. We also wish to thank Horace Moore for pointing out an error in an eariler version.

LEMMA 2. *No path of type CCCC is an R-geodesic.*

Proof. (See fig. 4.) Assume otherwise and let X be a path of type $CCCC$ which is an R-geodesic. Let P_0 and P_4 be the initial and terminal points of X. X consists of four arcs of circles. Let the first arc of X be an arc of the circle S_1 with center Q_1 and let the last arc of X be an arc of the circle S_4 with center Q_4. It is no loss of generality to assume that $R = 1$, i.e., the radius of S_1 is 1. Let $2d$ be the distance between Q_1 and Q_4. Clearly $0 \leqq 2d \leqq 6$. It is no loss of generality to assume that S_1 is oriented clockwise. We may also assume that the plane has rectangular coordinates with the origin at Q_1. We may further assume that Q_4 has coordinates $(2d, 0)$. Let R_0 be the point $(0, 1)$. R_0 is on S_1. Let R_4 be the point $(2d, -1)$. R_4 is on S_4. Now let W be the collection of all paths Y of the type $CCCC$ with initial point P_0 and terminal point P_4 and where the first arc of Y is a clockwise oriented arc of the circle S_1 and where the last arc of Y is a counterclockwise oriented arc of the circle S_4. $Y = P_0P_1P_2P_3P_4$, where $P_{i-1}P_i$ is an oriented arc with length L_i of an oriented circle S_i with center Q_i for $i = 1, 2, 3, 4$ and where S_i is tangent to S_{i+1} at the point P_i for $i = 1, 2, 3$. Here S_1, S_4, P_0 and P_4 are fixed whereas S_2, S_3, P_1, P_2, P_3, L_1, L_2, L_3 and L_4 vary with Y. Let u_1 be the arc length of the clockwise oriented arc R_0P_1 of the circle S_1. Let u_2 and u_3 be defined by $u_1 + u_2 = L_2$ and $u_2 + u_3 = L_3$. Clearly

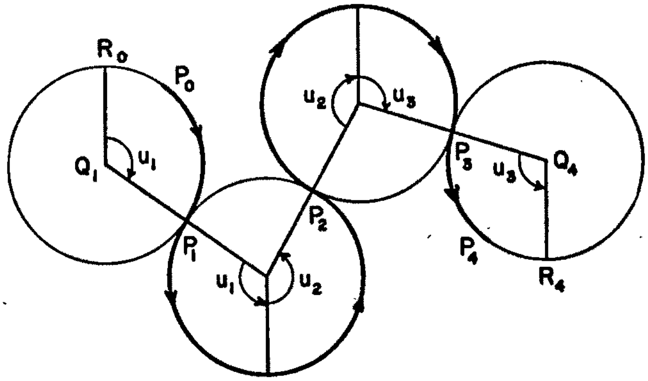

Figure 4.

$$L = L_1 + L_2 + L_3 + L_4$$
$$= (L_1 - u_1 + u_1) + (u_1 + u_2) + (u_2 + u_3) + (u_3 + L_4 - u_3)$$
$$= L_1 - u_1 + 2(u_1 + u_2 + u_3) + L_4 - u_3.$$

Furthermore, $L_1 - u_1$ and $L_4 - u_3$ are constants independent of Y in W. Hence, a necessary and sufficient condition for $L(Y)$ to attain its minimum at X is that $u_1 + u_2 + u_3$ attain its minimum at X. Clearly (u_1, u_2, u_3) is an admissible triad if and only if it satisfies the two constraints:

(1) $\sin u_1 + \sin u_2 + \sin u_3 = d$ and (2) $\cos u_1 - \cos u_2 + \cos u_3 = 0$.

There are now two possibilities for any point, (u_1, u_2, u_3), at which a minimum of $u_1 + u_2 + u_3$, subject to the two constraints, occurs: Either the cross product of the two gradient vectors

$$w_1 = (\cos u_1, \cos u_2, \cos u_3) \quad \text{and} \quad w_2 = (-\sin u_1, \sin u_2, -\sin u_3)$$

is the zero vector or $w_1 \times w_2 \neq 0$. Clearly

$$w_1 \times w_2 = (-\sin(u_2 + u_3), \sin(u_3 - u_1), \sin(u_1 + u_2)).$$

Suppose first that $w_1 \times w_2 = 0$. Then $\sin(u_1 + u_2) = 0$. Then $u_1 + u_2$ is a multiple of π. That is, L_2, the arc length of P_1P_2, is a multiple of π. Since X is assumed to be an R-geodesic of type $CCCC$, it is easy to see that L_2 is neither the zero multiple of π nor can L_2 be as large as 2π. Hence $L_2 = \pi$. Then part of X, namely $P_0P_1P_2P_3$ is a curve of type CCC, where the middle arc is of length π. But we have the following

SUBLEMMA. *No curve of type CCC, where the middle arc is of length greater than zero but not greater than πR, can be an R-geodesic.*

We omit the proof of this sublemma for it is quite similar to the proof of Case 1 of Lemma 1. This sublemma implies that $P_0P_1P_2P_3$ is not an R-geodesic. Hence $X = P_0P_1P_2P_3P_4$ could not be an R-geodesic. Therefore, we need only consider the case $w_1 \times w_2 \neq 0$. Hence, we may assume that the two constraints (1) and (2) determine a curve in the neighborhood of the point (u_1, u_2, u_3) at which the minimum of $u_1 + u_2 + u_3$ is attained, and that $w_1 \times w_2$ is tangent to the curve. Let m = minimum of $u_1 + u_2 + u_3$ subject to the constraints. Then the plane $u_1 + u_2 + u_3 = m$ is tangent to the constraint curve at the point at which the minimum is attained. That is, this plane contains the tangent vector $w_1 \times w_2$ at this point. Equivalently, the vector $(1, 1, 1)$ is orthogonal to $w_1 \times w_2$. Hence

$$-\sin(u_2 + u_3) + \sin(u_3 - u_1) + \sin(u_1 + u_2) = 0.$$

It is not difficult to show that if $\sin(A + B) = \sin A + \sin B$, then either A or B or $A + B$ is a multiple of 2π. Thus, either $u_2 + u_3$ or $u_3 - u_1$ or $u_1 + u_2$ is a multiple of 2π. But $u_1 + u_2 = L_2$, the arc length of P_1P_2.

Hence $0 < u_1 + u_2 < 2\pi$. Therefore $u_1 + u_2$ is not a multiple of 2π. Similarly $u_2 + u_3$ is not. Hence $u_3 - u_1$ is a multiple of 2π. Thus at the critical point, $w_1 \times w_2 = (\sin(v_2 + v_1), 0, \sin(v_2 + v_1))$. Since $w_1 \times w_2 \neq 0$, the first component of the tangent $w_1 \times w_2$ is unequal to zero. Therefore, the constraint curve can be parametrized by u_1. at least in a neighborhood of the critical point. In the sequel, all differentiations will be with respect to u_1 in a neighborhood of the critical point. Differentiating the two constraints we get:

$$u_1' \cos u_1 + u_2' \cos u_2 + u_3' \cos u_3 = 0, \qquad -u_1' \sin u_1 + u_2' \sin u_2 - u_3' \sin u_3 = 0$$

Furthermore, at the critical point, $u_1 + u_2 + u_3$ is a minimum, and hence $u_1' + u_2' + u_3' = 0$. These three equations imply that at a critical point $u_2' \sin(u_1 + u_2) = 0$. Since $\sin(u_1 + u_2) \neq 0$, we conclude that $u_2' = 0$. Hence $u_3' = -u_1' = -1$. We next observe that a necessary condition for $u_1 + u_2 + u_3$ to have a minimum at a regular point of the constraint curve is that the inner product of $r = (1, 1, 1)$ with the curvature vector be non-negative. Let $Z(s) = (u_1(s), u_2(s), u_3(s))$ be a parametrization of the constraint curve in a neighborhood of the critical point, where s is arc length for the curve. Clearly dz/ds is the tangent vector. We may assume that $w_1 \times w_2(u_1) = b(s) dz/ds$, where $b(s) > 0$ and where $s = s(u_1)$ is a function of u_1. Hence $(w_1 \times w_2)' = b(s)(d^2z/ds^2)s' + (db/ds)s'(dz/ds)$. At the critical point, dz/ds is perpendicular to r. Hence $(r, (w_1 \times w_2)') = b(s)s'(r, d^2z/ds^2)$. Since $b(s) > 0$, we conclude that a necessary condition for $u_1 + u_2 + u_3$ to have a minimum is that $s'(r, (w_1 \times w_2)') \geqq 0$. Clearly

$$\begin{aligned}&(w_1 \times w_2)' \\ &= (-\cos(u_2 + u_3)(u_2' + u_3'), \cos(u_3 - u_1)(u_3' - u_1'), \cos(u_1 + u_2)(u_1' + u_2')).\end{aligned}$$

But at the critical point, $u_1 = u_3$, $u_2' = 0$, $u_1' = 1$, $u_3' = -1$. Hence

$$(w_1 \times w_2)' = (\cos(u_2 + u_1), -2, \cos(u_1 + u_2)).$$

Therefore $(r, (w_1 \times w_2)') = 2\cos(u_1 + u_2) - 1$. Hence, a necessary condition for a minimum is that $2s'(\cos(u_1 + u_2) - 1) \geqq 0$. Hence, a necessary condition for a minimum is either $s' \leqq 0$ or $u_1 + u_2$ a multiple of 2π. Now we observe that the first component of $w_1 \times w_2$ equals the first component of $b(s)dz/ds$. Hence $-\sin(u_2 + u_3) = b(s) du_1/ds$. Since $b(s) > 0$, we have $\sin(u_2 + u_3) \geqq 0$ if and only if $du_1/ds \leqq 0$. Furthermore, since $w_1 \times w_2 \neq 0$ at a regular point, $\sin(u_2 + u_3) \neq 0$ there. Hence

$$\sin(u_2 + u_3) > 0 \Leftrightarrow du_1/ds \leqq 0 \Leftrightarrow ds/du_1 = s' \leqq 0.$$

We again recall that $u_3 = u_1$ at a critical point. Hence, a necessary condition for a minimum of $u_1 + u_2 + u_3$ subject to the two constraints is that $0 \leqq u_1 + u_2 \leqq \pi$. Now $X = P_0P_1P_2P_3P_4$, where L, the arc length of P_1P_2, is $u_1 + u_2$. By the sublemma, $P_0P_1P_2P_3$ is not an R-geodesic. Hence, neither is X. This completes the proof of the lemma.

We have now established our main result:

THEOREM I. *Every planar R-geodesic is necessarily a continuously differentiable curve which is either* (1) *an arc of a circle of radius R, followed by a line segment, followed by an arc of a circle of radius R; or* (2) *a sequence of three arcs of circles of radius R; or* (3) *a subpath of a path of type* (1) *or* (2).

COROLLARY. *There exists an R-geodesic of type CCC.*

Proof. Consider the problem of making a U-turn. That is let X be an R-geodesic whose initial and terminal positions are the same, and whose terminal tangent vector is the negative of its initial tangent vector. Let P be the finite set which consists of the paths of types (1), (2), and (3) referred to in Theorem 1 with the prescribed boundary conditions. In P there are two paths of type CCC. It is at most an elementary calculation to show that no path in P has a length less than either of these. Hence, by Theorem 1, these two paths are R-geodesics. This completes the proof of the corollary.

7. Non-existence of paths of minimal length. Let u, v, U and V be vectors in real n-dimensional Euclidean space, E_n. Let $\| U \| = \| V \| = 1$ and let $R > 0$. Let $C^* = C^*(n, u, U, v, V, R)$ be the collection of all curves X defined on a closed interval $[0, L]$, where $L = L(X)$ varies with X such that: $X(s) \in E_n$ for $0 \leqq s \leqq L$; $\| X'(s) \| = 1$; $X''(s)$ exists everywhere and $\| X''(s) \| \leqq R^{-1}$ for $0 \leqq s \leqq L$; $X(0) = u$, $X'(0) = U$, $X(L) = v$, and $X'(L) = V$.

PROPOSITION 14. *There exist u, U, v, V and R such that the infimum of the length of the curves X in* $C^* = C^*(2, u, U, v, V, R)$ *is not attained.*

Proof. Let $u = (0,0)$, $U = (0,1)$, $v = (5,0)$, $V = (0,-1)$ and $R = 1$. It is easy to see that there exists a curve Y of type ALA of length $\pi + 3$ such that $Y \in C = C(2, u, U, v, V, R)$. Proposition 9 implies that Y is the unique curve of minimal length in C. It is clear that C^* is a subset of C and that Y is not an element of C^*. To complete the proof of the proposition it is sufficient to show that for any $\epsilon > 0$, there exists $X \in C^*$ of length less than $\pi + 3 + 4\epsilon$. We will define X uniquely on an interval $[0, L_\epsilon]$ by specifying L_ϵ, $X(0)$, $X'(0)$ and the oriented curvature $k(s)$ for $0 \leqq s \leqq L_\epsilon$. Let $X(0) = u$, $X'(0) = U$, and $k(s) = 1$ for $0 \leqq s \leqq \frac{1}{2}\pi - \epsilon$. Let $k(s)$ be linear for s between $\frac{1}{2}\pi - \epsilon$ and $\frac{1}{2}\pi + \epsilon$, and let $k(\frac{1}{2}\pi + \epsilon) = 0$. Now let d be the first coordinate of the point $X(\frac{1}{2}\pi + \epsilon)$. We can now continue to define k. Let $k(s) = 0$ for $\frac{1}{2}\pi + \epsilon \leqq s \leqq 5 + \frac{1}{2}\pi + \epsilon - 2d$. Let $k(s)$ be linear for s between $5 + \frac{1}{2}\pi + \epsilon - 2d$ and $5 + \frac{1}{2}\pi + 3\epsilon - 2d$. Lastly, let $k(s) = 1$ for $5 + \frac{1}{2}\pi + 3\epsilon - 2d \leqq L_\epsilon$, where $L_\epsilon = 5 + \pi + 2\epsilon - 2d$. Thus X is uniquely defined. Since both the curvature k and its antiderivative can easily be integrated by elementary means, it is at most an elementary calculation to establish that X indeed is in C^*, and that the length L_ϵ of X is indeed less than $\pi + 3 + 4\epsilon$. We omit the details. The intuitive idea is that X was constructed so as to be a twice differentiable curve which approximates Y in an appropriate sense. This completes the proof.

In the course of the proof, we showed that the particular R-geodesic Y in $C(2, u, U, v, V, R)$ had the property that given any $\epsilon > 0$, there exists an X in $C^*(2, u, U, v, V, R)$ whose length differs from the length of Y by a quantity $f(\epsilon)$ which goes to zero with ϵ. It might be conjectured that every R-geodesic has this property. The following is a counterexample to this conjecture. Let Y be a continuously differentiable curve which consists of an arc of length $\frac{1}{2}\pi$ of a counterclockwise oriented circle of radius 1, followed by an arc of length $\frac{1}{2}\pi$ of a clockwise oriented circle of radius 1. We omit the proof that such a Y is indeed a counterexample.

CARNEGIE INSTITUTE OF TECHNOLOGY.

REFERENCES.

[1] L. M. Graves, *The Theory of Functions of Real Variables*, New York and London, 1946.

[2] E. Schmidt, "Über das Extremum der Bogenlänge einer Raumkurve bei vorgeschreibenen Einschränkungen ihrer Krümmung," *Sitzungsberichte Akad. Berlin* (1925), pp. 485-490.

[3] A. Schur, "Über die Schwarzsche Extremaleigenschaft des Kreises unter den Kurven konstanter Krümmung," *Mathematische Annalen*, vol. 83 (1921), pp. 143-148.

RELATIVE CHARACTERISTIC CLASSES.*

By MICHEL A. KERVAIRE.

1. Introduction. The main purpose of this paper [1] is to prove a lemma (Lemma (1.2) below) conjectured in [8].

In the proof, we shall make use of a not quite classical form of Whitney duality, involving Stiefel-Whitney characteristic classes which have to be considered as *relative* cohomology classes. Since these slightly generalized characteristic classes may have some interest for themselves, the present paper is divided into two parts as follows.

In Part I, an attempt is made to give a systematic treatment of relative characteristic classes. Beside Stiefel-Whitney classes, relative Chern and Pontryagin characteristic classes will also be considered. It will be seen that most of the properties of the usual characteristic classes may be adapted to hold for the relative classes. In particular, the relative classes satisfy a generalized Whitney duality theorem and Wu's theorem [16] remains true if suitably stated. The fact that Wu's theorem may be extended to the case of a manifold with boundary was communicated to me by R. Thom and was the starting point of the proof of Lemma (1.2). According to R. Thom, this extension of Wu's theorem was first known to H. Cartan, who proved it using (Φ)-cohomology (unpublished). For our purpose, it will be sufficient to reduce (by Lemma (6.1)) the extended Wu's theorem to the ordinary one, thus avoiding (Φ)-cohomology. The proof of the generalized Whitney duality will be based on the interpretation of the relative characteristic classes as symmetric functions. The original author's proof was very cumbersome and will be omitted. The proof given here is due to A. Borel and is reproduced with his permission.

Part II will be concerned with the following situation considered in [8]: Let M_d be a differentiable closed manifold imbedded [2] into some euclidean

---

* Received January 4,. 1957.

[1] The paper has been completed as the author was under National Science Foundation research contract. The author is also grateful to the Research Commission of Berne University (Switzerland) and to the Swiss Federal School of Technology for grants made available during the preparation of this paper.

[2] All manifolds considered are of class C^{∞}. Imbedding will mean regular imbedding (and similarly for immersion).

space E_{d+n}, and assume that there exists a continuous field $\boldsymbol{F}_n$ of n-frames (n mutually orthogonal unit vectors) *normal* to M_d in E_{d+n}. To such a pair $(M_d; \boldsymbol{F}_n)$ we attach

(a) a map $\omega\colon M_d \to V_{d+n,n}$ of M_d into the Stiefel manifold of n-frames with base point at the origin in E_{d+n}: the map ω is defined by

$$\omega(x) = \{\boldsymbol{v}_1(x), \boldsymbol{v}_2(x), \cdots, \boldsymbol{v}_n(x)\},$$

where $\boldsymbol{v}_1(x), \cdots, \boldsymbol{v}_n(x)$, are the vectors based at the origin in E_{d+n} and parallel to the vectors of $\boldsymbol{F}_n$ at x; and we also attach

(b) a map $f\colon S_{d+n} \to S_n$ of the $(d+n)$-dimensional sphere into the n-sphere defined as follows: Take a tubular neighborhood U of M_d in E_{d+n}. Any point $u \in U$ lies in a uniquely determined n-plane N_x normal to M_d at a (uniquely defined) point $x \in M_d$. Using the coordinate system in N_x which is defined by the mutually orthogonal unit vectors of $\boldsymbol{F}_n$ at x, we attach coordinates $y_1, \cdots, y_n$ to the point u. It may be assumed that $\sum_i (y_i)^2 = 1$, if and only if u lies on the boundary of U. The definition of f will involve the mapping

$$r\colon (B_n, \partial B_n) \to (S_n, q^*)$$

of the n-ball B_n onto the n-sphere S_n given (for instance) by the formula

$$(1.1)\quad r(y_1, \cdots, y_n) = (1-2y^2, 2y_1(1-y^2)^{\frac{1}{2}}, 2y_2(1-y^2)^{\frac{1}{2}}, \cdots, 2y_n(1-y^2)^{\frac{1}{2}}),$$

where $y^2 = \sum_k (y_k)^2$ and $q^* \in S_n$ is the point with coordinates $(-1, 0, \cdots, 0)$. Identifying now S_{d+n} with $E_{d+n} + \infty$, the desired mapping $f\colon S_{d+n} \to S_n$ is given by

$$f(u) = r(y_1, \cdots, y_n) \text{ for } u \in U, \qquad f(x) = q^* \text{ for } x \in S - U.$$

The homotopy class of the map ω (defined under (a) above) is determined[3] by the generalized *curvatura integra* c which represents the homology class of the cycle $\omega(M_d)$ in $H_d(V_{d+n,n}; \boldsymbol{Z})$. The number c is an integer for d even or $n = 1$ and a remainder mod 2 for d odd ($n > 1$). Define γ by $\gamma = c - \chi^*(M_d)$, where $\chi^*(M_d)$, the semi-characteristic of M_d, is equal to $\frac{1}{2}\chi(M_d)$ for d even and to $\sum_{i=0}^{s-1} (-1)^i p_i(M_d)$ for d odd, $p_i(M_d)$ being then the rank of $H_i(M_d; \boldsymbol{Z}_2)$, and $2s = d + 1$.

---

[3] Recall that the Stiefel manifold of n-frames in $(d+n)$-space is $(d-1)$-connected and its d-dimensional integer homology group is infinite cyclic, or cyclic of order 2, depending on whether d is even or $n = 1$, or d is odd and $n > 1$ respectively.

It has been proved in [8] (Théorème II) that if a manifold M_d' with normal n-frame field $\boldsymbol{F}_n'$ in E_{d+n} leads (by procedure (b)) to a map f'; $S_{d+n} \to S_n$ homotopic to f, then $\gamma = \gamma'$, i. e., $c - \chi^*(M_d) = c' - \chi^*(M_d')$, this formula being valid only mod 2 for d odd.

Actually each homotopy class in $\pi_{d+n}(S_n)$ contains maps $f\colon S_{d+n} \to S_n$ obtained by the procedure described under (b) and γ is a homomorphism of $\pi_{d+n}(S_n)$ into $\boldsymbol{Z}$ or $\boldsymbol{Z}_2$ according as d is even or odd. It has been proved in [8] (Théorème IV) that, for d even, γ is always zero.

Another homotopy invariant associated to f which will play a role in the present paper is Hopf's invariant as generalized by Steenrod [11]: Consider the cell complex $K = S_n \cup e_{d+n+1}$ obtained by attaching the cell e_{d+n+1} to S_n by the given map f, then Steenrod's generalization of Hopf's invariant, which will be denoted by $h(f)$, is the remainder mod 2 defined by

$$Sq^{d+1}(u) = h(f) \cdot v,$$

where u and v are the generators of $H^n(K; \boldsymbol{Z}_2)$ and $H^{n+d+1}(K; \boldsymbol{Z}_2)$ respectively and Sq^{q+1} is the Steenrod square which raises the degree by $d+1$.

Each of the invariants $h(f)$ and $\gamma(f)$ has the following properties which can be verified easily (see [8]) for $\gamma(f)$ and were proved by Steenrod ([11], § 18) for $h(f)$:

(1) It is a homomorphism of $\pi_{d+n}(S_n)$ into $\boldsymbol{Z}_2$ defined for every $d \geqq 1$ and $n \geqq 1$.

(2) It vanishes for d even.

(3) It takes the same value on a homotopy class and on its Freudenthal suspension.

(4) It is zero for every composition map $g \circ f\colon S_p \to S_r$, where $f\colon S_p \to S_q$, $g\colon S_q \to S_r$, provided that $p > q > r$.[4]

(5) If S_d is parallelizable, it takes the value 1 on the standard Hopf's map $s\colon S_{2d+1} \to S_{d+1}$ with Hopf's invariant 1.

It is not unlikely that properties (1)-(5) should characterize completely $h(f)$. This proves to be true for $d \leqq 7$, even with property (4) omitted.[5] I have no proof of this conjecture for general d. However, using the explicit definitions of $h(f)$ and $\gamma(f)$, we shall prove below the following lemma, which was conjectured in [8]:

LEMMA (1.2). *Using the above notations,* $\gamma(f) = h(f)$.

---

[4] This fact has not been proved for γ in [8] but is easily seen.

[5] See [8], page 242.

The use which can be made of relative characteristic classes to prove this lemma will become apparent during the proof in Section 8.

I am indebted and wish to express my gratitude to A. Borel and R. Thom for many fruitful discussions during the preparation of the present paper.

PART I. Relative characteristic classes.

2. Definition. We shall treat first Stiefel-Whitney classes. The relative Chern and Pontryagin classes may be obtained similarly and will be discussed briefly in an Appendix (§ 11). The coefficients will be the remainder mod 2, except in § 11 (and § 6).

Let $\mathfrak{B} = (B, p, K, S_{n-1}, \boldsymbol{O}(n))$ be a sphere-bundle over the simplicial complex K with the orthogonal group of n variables $\boldsymbol{O}(n)$ as structural group. Denote by $\mathfrak{B}^q = (B^q, p^q, K, V_{n,n-q}, \boldsymbol{O}(n))$ the bundle associated to $\mathfrak{B}$ with fibre the Stiefel manifold $V_{n,n-q}$ of $(n-q)$-frames (based at a fixed point) in euclidean n-space.

Let L be a subcomplex of K and assume that a cross-section θ^r over L is given in the associated bundle $\mathfrak{B}^r$. This section induces (by the projection $B^r \to B^q$) cross-sections θ^q over L in the associated bundle $\mathfrak{B}^q$ for $q \geqq r$. Roughly speaking, θ^r defines an $(n-r)$-vectorfield $\boldsymbol{F}_{n-r}$ over L, and θ^q is given by the $(n-q)$-vectorfield consisting of the first $(n-q)$ vectors of $\boldsymbol{F}_{n-r}$.

Let W^{q+1} be the $(q+1)$-dimensional Stiefel-Whitney class of the bundle $\mathfrak{B}$. Suppose $q \geqq r$. A representative w^{q+1} of W^{q+1} may be obtained by the usual stepwise extension process over $K^0 \cup L, K^1 \cup L, K^2 \cup L, \cdots, K^q \cup L$ of the cross-section θ^q in $\mathfrak{B}^q$ induced by θ^r over L. The *requirement* that the cross-section over K^q in $\mathfrak{B}^q$ should coincide over L with the given section θ^q leads to a representative w^{q+1} of W^{q+1} which takes the value zero on every $(q+1)$-simplex of L. The cocycle w^{q+1} is thus a representative of a *relative* cohomology class $W_R^{q+1} \in H^{q+1}(K, L; \boldsymbol{Z}_2)$ defined for $q \geqq r$, which will be called the $(q+1)$-dimensional *relative characteristic* Stiefel-Whitney class mod L corresponding to θ^r.

W_R^{q+1} does not depend on the choice of the extension of θ^q over the 0-, 1-, $\cdots$, q-simplexes of K-L (see [12], 33.5). It does, however, depend, in general, on the choice of the given cross-section over L. Let θ^0 and θ^1 be two cross-sections over L in $\mathfrak{B}^r$ and let θ^{0q}, θ^{1q} be their projections in $\mathfrak{B}^q$ $(q \geqq r)$. The stepwise attempt to make the cross-sections θ^{0q} and θ^{1q} coincide meets with an obstruction in dimension q on L. Let $b^q \in H^q(L)$ be the obstruction cohomology class. It is easily seen, that δb^q is the difference of the $(q+1)$-dimensional Stiefel-Whitney classes corresponding to θ^0 and θ^1, where δ is the coboundary operator of the cohomology sequence:

$$\cdots \leftarrow H^{q+1}(K) \leftarrow H^{q+1}(K,L) \xleftarrow{\delta} H^q(L) \leftarrow H^q(K) \leftarrow \cdots.$$

3. Naturality. Suppose we are given two principal $\boldsymbol{O}(n)$-bundles $\mathfrak{B}$ and $\mathfrak{B}'$ over simplicial complexes K, K' respectively, such that $\mathfrak{B}$ is induced from $\mathfrak{B}'$ by a map $f\colon K \to K'$ which we assume to be simplicial.

Let L and L' be subcomplexes of K and K' respectively, such that $f(L)$ is a subcomplex of L'. Suppose that cross-sections θ^r and θ'^r over L and L' are given in the associated bundles $\mathfrak{B}^r$ and $\mathfrak{B}'^r$ with fibre $V_{n,n-r}$, such that $h\theta^r(x) = \theta'^r f(x)$ for every $x \in L$ (h is the bundle map covering f).

Then, for $q \geqq r$, the relative characteristic Stiefel-Whitney classes W_R^{q+1} and W'^{q+1}_R of the two bundles are both defined.

LEMMA (3.1). *We have* $W_R^{q+1} = f^*(W'^{q+1}_R)$, *where* f^* *is the dual homomorphism* $f^*\colon H(K',L';\boldsymbol{Z}_2) \to H(K,L;\boldsymbol{Z}_2)$ *induced by* $f\colon (K,L) \to (K',L')$. (See [12], 32.7).

Choose an extension over $K'^q \cup L'$ of the cross-section θ'^q in $\mathfrak{B}'^q$ given over L'. Define W'^{q+1}_R using this extension. Define θ^q over $K^q \cup L$ as the reverse image by h of the cross-section θ'^q. By assumption, this definition is consistent with the given cross-section over L in $\mathfrak{B}^q$ and the extended θ^q may be used to define W_R^{q+1}. Let s be a $(q+1)$-simplex of K. If $f(s) = 0$, $|f(s)|$ is a subset of the q-dimensional skeleton of K', thus θ^q may be defined over s and $w^{q+1}(s) = w'^{q+1}(fs) = 0$. If $f(s) \neq 0$, the restriction of f on s is a homeomorphism, and $w^{q+1}(s) = w'^{q+1}(fs)$ follows from $h\theta^q \mid \dot{s} = \theta'^q f \mid \dot{s}$, together with the fact that h induces the identity $h_*\colon \boldsymbol{Z}_2 \to \boldsymbol{Z}_2$ (identifying $H_q(V_{n,n-q};\boldsymbol{Z}_2)$ with $\boldsymbol{Z}_2$). Thus, for the cohomology classes of w^{q+1} and w'^{q+1}, $W_R^{q+1} = f^*(W'^{q+1}_R)$.

4. The Whitney duality. Let $\mathfrak{B}_i$ be two principal $\boldsymbol{O}(n_i)$-bundles $(i = 1, 2)$ over the same simplicial complex K, and suppose that cross-sections $\theta_1^{r_1}$ and $\theta_2^{r_2}$ over subcomplexes L_1, L_2 of K are given in the corresponding associated bundles $\mathfrak{B}_1^{r_1}$, $\mathfrak{B}_2^{r_2}$.

Let $\mathfrak{B} = \mathfrak{B}_1 \oplus \mathfrak{B}_2$ be the Whitney sum of $\mathfrak{B}_1$ and $\mathfrak{B}_2$. The bundle $\mathfrak{B}$ is an $\boldsymbol{O}(n_1 + n_2)$-bundle. The cross-sections $\theta_1^{r_1}$, $\theta_2^{r_2}$ induce over $L = L_1 \cap L_2$ (where they are both defined) a cross-section θ^r in the associated bundle $\mathfrak{B}^r$

with fibre $V_{n,n-r}$ $(n = n_1 + n_2, r = r_1 + r_2)$. We shall refer to θ^r as the *sum* of the given cross-sections $\theta_1^{r_1}$ and $\theta_2^{r_2}$.

Using the sum cross-section θ^r over L, we define the relative Stiefel-Whitney classes W_R^{q+1} of $\mathfrak{B} \bmod L$ for $q \geqq r$. Denote by X_R^{k+1} and Y_R^{l+1} the relative Stiefel-Whitney classes of $\mathfrak{B}_1$ and $\mathfrak{B}_2$ corresponding to the cross-sections $\theta_1^{r_1}$, $\theta_2^{r_2}$. They are defined for $k \geqq r_1$ and $l \geqq r_2$ respectively.

In the Theorem (4.1) below, expressing Whitney duality for relative classes, the classes X_R^{k+1}, Y_R^{l+1} which are relative classes $\bmod L_1$ and $\bmod L_2$ respectively are regarded as relative classes $\bmod L$. Precisely, we write X_R^{k+1}. meaning the image of X_R^{k+1} by the homomorphism $H^*(K, L_1) \to H^*(K, L)$ induced by the inclusion $(K, L) \to (K, L_1)$, and similarly for Y_R^{l+1}.

THEOREM (4.1). *The Whitney duality holds for relative characteristic Stiefel-Whitney classes in the following form: For $q \geqq r$, we have*

$$W_R^{q+1} = X_R^{q+1} + X_R^q \cdot Y^1 + \cdots + X_R^{r_1+1} \cdot Y^{q-r_1} + \\ + X^{r_1} \cdot Y_R^{q-r_1+1} + \cdots + Y_R^{q+1}.$$

Notice that some absolute (usual) characteristic classes occur in the right hand side of the above formula. However, in each cup-product $X^a \cdot Y^b$ with $a + b - 1 = q \geqq r_1 + r_2$, either $a - 1 \geqq r_1$ or $b - 1 \geqq r_2$ (or both), because $a \leqq r_1$ and $b \leqq r_2$ would imply $a + b \leqq r_1 + r_2$. Therefore, in each product $X^a \cdot Y^b$, at least one of the classes X^a or Y^b is a relative class and so is every product in the right hand side of (4.1).

The proof of the above theorem will be carried out by showing that the relative characteristic classes may be equivalently defined as symmetric functions (Theorem (5.1)). This alternative definition in turn implies immediately the above duality theorem.

5. Relative characteristic classes as symmetric functions. Proof of Whitney duality. Let us recall Borel's definition of the (usual) characteristic classes [4]. Let $\mathfrak{B} = (E, p, K, \boldsymbol{O}(n))$ be a principal $\boldsymbol{O}(n)$-bundle over K. Let $\boldsymbol{Q}(n)$ denote the subgroup of $\boldsymbol{O}(n)$ consisting of the diagonal matrices $(e_i\delta_{ij})$, with $e_i = +1$ or -1. The space E is also the bundle space of a fibre bundle with fibre $\boldsymbol{Q}(n) = \boldsymbol{O}(1) \times \boldsymbol{O}(1) \times \cdots \times \boldsymbol{O}(1)$ (n factors), which is a covering space since $\boldsymbol{Q}(n)$ is discrete. The base space $\bar{K} = E/\boldsymbol{Q}(n)$ of this bundle is called the space of flags over K. The space $\bar{K}$ is the bundle space of a bundle with fibre $\boldsymbol{F}(n) = \boldsymbol{O}(n)/\boldsymbol{Q}(n)$ and base space K. Let $\rho : \bar{K} \to K$ be the projection.

The bundle $\mathfrak{E} = (E, \pi, \bar{K}, \boldsymbol{Q}(n))$ is the Whitney sum of n bundles $\mathfrak{E} = \mathfrak{E}^1 \oplus \mathfrak{E}^2 \oplus \cdots \oplus \mathfrak{E}^n$, where $\mathfrak{E}^i$ is a principal bundle over $\bar{K}$ with structural group $\boldsymbol{O}(1) \cong \boldsymbol{Z}_2$, thus a two-fold covering. Let $x_i \in H^1(\bar{K}; \boldsymbol{Z}_2)$ be the 1-dimensional (only non-zero positive dimensional) Stiefel-Whitney classes of $\mathfrak{E}^i$, $i = 1, 2, \cdots, n$, defined, for instance, as obstruction to the construction of a cross-section in $\mathfrak{E}^i$ over the 1-dimensional skeleton of $\bar{K}$. We have the

THEOREM (A. Borel). *The dual homomorphism $\rho^*: H^*(K) \to H^*(\bar{K})$ is a monomorphism and the ρ^*-image of $H^*(K)$ contains the symmetric functions of the variables $x_1, x_2, \cdots, x_n$.*

It is then legitimate to define the characteristic class W^q of the bundle $\mathfrak{B}$ by the formula $\rho^*(W^q) = S^q(x_1, \cdots, x_n)$, where $S^q(x_1, \cdots, x_n)$ denotes the elementary symmetric function of degree q in the variables $x_1, \cdots, x_n$.

A. Borel has proved in [4] (Théorème 5.1) that the class W^q defined in this way coincides with the characteristic class defined as obstruction.

We come back to relative classes: Suppose a cross-section θ^r is given in the bundle $\mathfrak{B}^r = (E^r, K, V_{n,n-r}, \boldsymbol{O}(n))$ associated to $\mathfrak{B}$ over a subcomplex L of K. Consider the space of flags $\bar{K} = E/\boldsymbol{Q}(n)$ over K. The section θ^r determines a subspace $\bar{L}$ of $\bar{K}$ as follows: Regarding $\mathfrak{B}$ as induced by a map $f: K \to B_{\boldsymbol{O}(n)}$, $f(x)$, $x \in K$, is a non-oriented n-plane in euclidean space of large dimension. A point of E consists of a point $x \in K$, together with an n-frame $v_1, v_2, \cdots, v_n$ in $f(x)$ (see [12], 10.2). Thus a point of $\bar{K}$ may be represented by $\{x; d_1, d_2, \cdots, d_n\}$, where $x \in K$ and $d_1, d_2, \cdots, d_n$ is an ordered set of mutually orthogonal straight lines in $f(x)$. The set $\bar{L}$ consists of those points $\{x; d_1, \cdots, d_n\}$ of $\bar{K}$ such that $x \in L$ and $d_{r+1}, \cdots, d_n$ carry the $(n-r)$ vectors of θ^r.

Let $x_1, \cdots, x_n \in H^1(\bar{K}; \boldsymbol{Z}_2)$ be, as before, the 1-dimensional characteristic classes of the two-fold coverings $\mathfrak{E}^1, \mathfrak{E}^2, \cdots, \mathfrak{E}^n$ over $\bar{K}$, the Whitney sum of which is the bundle $(E, \pi, \bar{K}, \boldsymbol{Q}(n))$. Because $\mathfrak{E}^{r+1}, \cdots, \mathfrak{E}^n$ admit cross-sections over $\bar{L}$ given by θ^r, the $(n-r)$ last x_i, $i = r+1, r+2, \cdots, n$, may be defined as *relative* characteristics classes $\operatorname{mod} \bar{L}$ (obstruction to extending over the 1-dimensional skeleton of $\bar{K}$ the cross-section in $\mathfrak{E}^i$, $r+1 \leqq i \leqq n$, already given over $\bar{L}$). Because in any product of $(q+1)$ distinct factors from $x_1, \cdots, x_n$ with $q \geqq r$, at least one of the last $n-r$ must occur, it follows that, for $q \geqq r$, the elementary symmetric function $S^{q+1}(x_1, \cdots, x_n)$ may be (and will be) defined as a relative cohomology class, which we shall denote by $S_R^{q+1}(x_1, \cdots, x_n)$, using the relative $x_{r+1}, \cdots, x_n$.

THEOREM (5.1). (a) *The homomorphism* $\rho_R^*: H^*(K,L) \to H^*(\bar{K},\bar{L})$ *is a monomorphism and* (b) $\rho_R^*(W_R^{q+1}) = S_R^{q+1}(x_1,\cdots,x_n)$ *for* $q \geqq r$, *where* W_R^{q+1} *is the relative characteristic class* mod L *corresponding to the cross-section* θ^r.

The proof of this theorem which will be given below is due to A. Borel. In the first formulation of this paper, the point (b) was proved using an inductive argument (on n) and the special case of relative Whitney duality in which one of the bundles involved in the Whitney sum is a two-fold covering. This special case of Whitney duality was proved directly using the definition of characteristic classes as obstruction, which is rather cumbersome. Futhermore, the point (a) of Theorem (5.1) could not be obtained by this method. The Lemma (5.2) below is also due to A. Borel and was unknown to the author.

The Whitney duality formula (4.1) is an immediate consequence of Theorem (5.1) and of the identity

$$S_R^{q+1}(x_1,\cdots,x_m,y_1,\cdots,y_n) = \sum_{a+b=q+1} S^a(x_1,\cdots,x_m)\cdot S^b(y_1,\cdots,y_n),$$

where each product in the right hand sum is a relative class (at least one factor in each product is a relative class if the left hand side is).

Before we proceed to the proof of Theorem (5.1), we give a property of the relative Stiefel-Whitney classes, which will be needed for this proof.

Let L be a subcomplex of $B_{\boldsymbol{O}(n)}$ and θ^r a cross-section over L in the associated bundle with fibre $V_{n,n-r}$. The cross-section θ^r induces cross-sections θ^q over L in every associated bundle with fibre $V_{n,n-r}$ for $q \geqq r$. The bundle space of the associated bundle with fibre $V_{n,n-r}$ is classifying space for $\boldsymbol{O}(q)$ and will consequently be denoted by $B_{\boldsymbol{O}(q)}$. The projection map $B_{\boldsymbol{O}(q)} \to B_{\boldsymbol{O}(n)}$ is the Borel map $\rho(\boldsymbol{O}(q),\boldsymbol{O}(n))$ corresponding to the inclusion $\boldsymbol{O}(q) \to \boldsymbol{O}(n)$. We write $\rho_{q,n}$, meaning $\rho(\boldsymbol{O}(q),\boldsymbol{O}(n))$, for notational convenience.

LEMMA (5.2). *The relative Stiefel-Whitney characteristic class* W_R^{q+1} *is the only non-zero element in* $H^{q+1}(B_{\boldsymbol{O}(n)},L;\boldsymbol{Z}_2)$ *belonging to the kernel of* $\rho_{q,n}^*: H^*(B_{\boldsymbol{O}(n)},L) \to H^*(B_{\boldsymbol{O}(q)},\theta^q L)$.

We first prove that W_R^{q+1} belongs to the kernel of $\rho_{q,n}^*$: The map $\rho_{q,n}: B_{\boldsymbol{O}(q)} \to B_{\boldsymbol{O}(n)}$ induces over $B_{\boldsymbol{O}(q)}$ as base space an $\boldsymbol{O}(q)$-bundle with fibre $V_{n,n-q}$ and the induced cross-section over $\theta^q L$ may be trivially extended all over $B_{\boldsymbol{O}(q)}$. By naturality the Stiefel-Whitney class corresponding to this cross-section is $\rho_{q,n}^*(W_R^{q+1})$. Since the cross-section may be extended, $\rho_{q,n}^*(W_R^{q+1}) = 0$.

In order to prove that W_R^{q+1} is the *only* non-zero element of dimension $q+1$ in the kernel of $\rho_{q,n}^*$, let us consider the following diagram, where the rows are the cohomology sequences of the pairs $(B_{O(q)}, \theta^q L)$ and $(B_{O(n)}, L)$ respectively:

$$\begin{tikzcd}
\cdots \arrow[r] & H^i(B_{O(q)}) \arrow[r, "j^*"] & H^i(\theta^q L) \arrow[r, "\delta"] \arrow[d, "\theta^*"] & H^{i+1}(B_{O(q)}, \theta^q L) \arrow[r] & H^{i+1}(B_{O(q)}) \arrow[r] & \cdots \\
\cdots \arrow[r] & H^i(B_{O(n)}) \arrow[r, "i^*"] \arrow[u, "\rho^*"] & H^i(L) \arrow[r, "\delta"] & H^{i+1}(B_{O(n)}, L) \arrow[r, "a^*"] \arrow[u, "\rho_{q,n}^*"] & H^{i+1}(B_{O(n)}) \arrow[r] \arrow[u, "\rho^*"] & \cdots
\end{tikzcd}$$

(coefficients in $\mathbf{Z}_2$). One has $H^*(B_{O(n)}; \mathbf{Z}_2) = \mathbf{Z}_2[W^1, W^2, \cdots, W^n]$, $H^*(B_{O(q)}; \mathbf{Z}_2) = \mathbf{Z}_2[W^1, W^2, \cdots, W^q]$ and the W^i for $i \leqq q$ correspond to each other by ρ^*. Thus, for $i \leqq q$, the homomorphism ρ^* is an isomorphism.

By the Five Lemma, it follows that for $i \leqq q$, the homomorphism $\rho_{q,n}^*$ is also an isomorphism (θ^* is an isomorphism in every dimension).

Let x be an element of the kernel of $\rho_{q,n}^*$ in $H^{q+1}(B_{O(n)}, L)$. By commutativity in the above diagram, a^*x is an element of the kernel of ρ^*. Therefore, by [4], Lemma 5.1, $a^*x = c \cdot W^{q+1}$ with $c = 0$ or 1. Thus $y = x + c \cdot W_R^{q+1}$ belongs to the kernels of both $\rho_{q,n}^*$ and a^*. By exactness, there exist elements z and t in $H^q(L)$ and $H^q(B_{O(q)})$ respectively, such that $\delta z = y$ and $j^*t = \theta^{*-1}z$. Since ρ^* is an epimorphism in every dimension, there exists a class $w \in H^q(B_{O(n)})$, such that $\rho^* w = t$. It follows that $y = \delta i^* w = 0$, by exactness.

This completes the proof of Lemma (5.2).

Notice that Lemma (5.2) suggests a new (more general) definition of the relative Stiefel-Whitney classes: Let A be a closed subset of $B_{O(n)}$ and suppose a cross-section θ^r over A is given in the bundle with fibre $V_{n,n-r}$ associated to the universal bundle over $B_{O(n)}$. The $(q+1)$-dimension universal relative Stiefel-Whitney class mod A corresponding to θ^r $(r \geqq q)$, may be defined as being the only non-zero element in the kernel of $\rho_{q,n}^*$: $H^*(B_{O(n)}, A) \to H^*(B_{O(q)}, \theta^q A)$. The proof of uniqueness runs as in Lemma (5.2), replacing L by A. To complete the definition, one has to show the existence of an element in kernel $\rho_{q,n}^*$, the image of which by a^* is the ordinary universal Stiefel-Whitney class and which is thus different from zero. Extension of this definition to the characteristic classes of a principal $\boldsymbol{O}(n)$-bundle over any compact finite dimensional space X is immediate. However, the naturality is less easy to prove in this general case. We omit the details here and shall treat relative Chern classes by this method (see Appendix).

Proof of Theorem (5.1). *Proof of* (a). This part is not concerned with characteristic classes. Let X be the base space (assumed to be a compact finite dimensional topological space) of an $\boldsymbol{O}(n)$-bundle induced by some map $X \to B_{\boldsymbol{O}(n)}$ and let $\bar{X}$ be the space of flags over X (denote by $\rho_X\colon \bar{X} \to X$ the projection). According to [4], Théorème 5.1, the fibre $\boldsymbol{F}(n) = \boldsymbol{O}(n)/\boldsymbol{Q}(n)$ is totally non-homologous to zero in $\bar{X}$ and thus $\rho_X{}^*\colon H^*(X) \to H^*(\bar{X})$ is a monomorphism.

Let A be a closed subspace of X and suppose that a cross-section θ^r over A is given in the associated bundle over X with fibre $V_{n,n-r}$. Let $\bar{A}$ be the subset of $\bar{X}$ the points of which are the sets $\{a; d_1,\cdots,d_n\}$, such that $a \in A$, and $d_{r+1},\cdots,d_n$ carry the $(n-r)$ vectors given over A by θ^r. Notice that $\bar{A}$ is homeomorphic to the space of the bundle $(\bar{A}, \rho_A, \boldsymbol{F}(r), \boldsymbol{O}(r))$ defined as follows: E being the space of the $\boldsymbol{O}(n)$-bundle over X, consider the fibering $(E/\boldsymbol{Q}(r), \rho_E, E/\boldsymbol{O}(r), \boldsymbol{F}(r), \boldsymbol{O}(r))$, where $\boldsymbol{Q}(r) \subset \boldsymbol{O}(r) \subset \boldsymbol{O}(n)$. The bundle $(\bar{A}, \rho_A, A, \boldsymbol{F}(r), \boldsymbol{O}(r))$ is induced by the cross-section $\theta^r\colon A \to E/\boldsymbol{O}(r)$. Therefore, by Borel's theorem, $\rho_A{}^*$ is also a monomorphism.

Consider the following commutative diagram in which the rows are the cohomology sequences of $(\bar{X}, \bar{A})$ and (X, A) respectively:

$$\begin{tikzcd}
\cdots & H^k(\bar{X}) \arrow[l] & H^k(\bar{X}, \bar{A}) \arrow[l, "\bar{j}^*"'] & H^{k-1}(\bar{A}) \arrow[l, "\delta"'] & H^{k-1}(\bar{X}) \arrow[l, "\bar{i}^*"'] & \cdots \arrow[l] \\
\cdots & H^k(X) \arrow[l] \arrow[u, "\rho_X{}^*"] & H^k(X, A) \arrow[l, "j^*"'] \arrow[u, "\rho_R{}^*"'] & H^{k-1}(A) \arrow[l, "\delta"'] \arrow[u, "\rho_A{}^*"'] & H^{k-1}(X) \arrow[l, "i^*"'] \arrow[u, "\rho_X{}^*"'] & \cdots \arrow[l]
\end{tikzcd} \tag{5.3}$$

We have to prove that $\rho_R{}^*$ is a monomorphism. Let $a \in H^k(X, A)$ be a cohomology class, such that $\rho_R{}^* a = 0$. Since $\bar{j}^* \rho_R{}^* a = \rho_X{}^* j^* a = 0$ and $\rho_X{}^*$ is a monomorphism, it follows that $j^* a = 0$. Thus by exactness, there exists a class $b \in H^{k-1}(A)$, such that $\delta b = a$. Because $\delta \rho_A{}^* b = \rho_R{}^* \delta b = \rho_R{}^* a = 0$, there exists (by exactness) an element $w \in H^{k-1}(\bar{X})$, such that $\bar{i}^* w = \rho_A{}^* b$. The desired conclusion $a = 0$ would be granted if we knew the existence of an element $x \in H^{k-1}(X)$, such that $i^* v = b$. Indeed, from the existence of v follows, by exactness, $a = \delta b = \delta i^* v = 0$.

It remains to prove the

LEMMA. *Let $b \in H^*(A)$ and $w \in H^*(\bar{X})$ be cohomology classes, such that $\rho_A{}^* b = \bar{i}^* w$, then there exists a cohomology class $v \in H^*(X)$, such that* $i^* v = b$ (Notations as in diagram (5.3)).

Proof. Let $x_1,\cdots,x_n$ denote, as before, the 1-dimensional characteristic classes of the two-fold coverings $\mathfrak{E}^1, \mathfrak{E}^2,\cdots,\mathfrak{E}^n$ over $\bar{X}$. By definition of $\bar{A}$, we have $\bar{i}^*x_a = y_a$ for $a = 1, 2, \cdots, r$ and $\bar{i}^*x_{r+b} = 0$ for $b = 1, \cdots, n-r$, where $y_1, \cdots, y_r$ denote the characteristic classes of the restriction over $\bar{A}$ of the two-fold coverings $\mathfrak{C}^1, \mathfrak{C}^2, \cdots, \mathfrak{C}^r$. The map $\bar{i}\colon \bar{A} \rightarrow \bar{X}$ restricted on a fibre (we denote this restriction again by $\bar{i}$) induces the inclusion $\boldsymbol{F}(r) \rightarrow \boldsymbol{F}(n)$ corresponding to the inclusion $(\boldsymbol{O}(r), \boldsymbol{Q}(r)) \rightarrow (\boldsymbol{O}(n), \boldsymbol{Q}(n))$. According to the results of A. Borel in [4] (Théorème 11.1), one has

$$H^*(\boldsymbol{F}(n); \boldsymbol{Z}_2) \cong \boldsymbol{Z}_2[x_1, \cdots, x_n]/(S^+(x_1, \cdots, x_n))$$

and similarly for $H^*(\boldsymbol{F}(r); \boldsymbol{Z}_2)$, where $(S^+(x_1, \cdots, x_n))$ denotes the ideal (in $\boldsymbol{Z}_2[x_1, \cdots, x_n]$) generated by the symmetric functions of positive degrees in the variables $x_1, \cdots, x_n$.

It is easily seen that there exists a basis $h_1, h_2, \cdots, h_t$ of $H^*(\boldsymbol{F}(n))$ over $\boldsymbol{Z}_2$ with the following properties:

(1) $h_1 = 1$, the h_i are monomials in the $x_1, \cdots, x_n$;

(2) $\bar{i}^*h_1, \bar{i}^*h_2, \cdots, \bar{i}^*h_s$ form a basis of $H^*(\boldsymbol{F}(r); \boldsymbol{Z}_2)$;

(3) $\bar{i}^*h_{s+1} = \bar{i}^*h_{s+2} = \cdots = \bar{i}^*h_t = 0$.

Such a basis may be obtained by writing down in some order, beginning with 1, all monomials in the variables $x_1, \cdots, x_r$ the degree of which does not exceed $\dim \boldsymbol{F}(r)$, followed by the other monomials in $x_1, \cdots, x_n$. By omitting in this list the monomials which are linearly dependent (modulo the ideal generated by $S^+(x_1, \cdots, x_n)$) of preceding ones, one obtains the desired basis $h_1, h_2, \cdots, h_t$.

By Borel's results, the spectral sequence of the fibering $\rho_X\colon \bar{X} \rightarrow X$ is trivial ($E_2 \cong E_\infty$). Furthermore, since we have a coefficient *field*, $\boldsymbol{Z}_2$, the term E_∞ is additively isomorphic to $H^*(\bar{X})$. Therefore,

$$H^*(\bar{X}) \cong H^*(X) \otimes H^*(\boldsymbol{F}(n))$$

is a module over $\rho_X{}^*H^*(X)$ with the basis $h_1, h_2, \cdots, h_t$. Similarly, $H^*(\bar{A})$ is a module over $\rho_A{}^*H^*(A)$ with the basis $\bar{i}^*h_1, \bar{i}^*h_2, \cdots, \bar{i}^*h_s$.

Any element $w \in H^*(\bar{X})$ admits a unique decomposition in the form

$$w = \sum_{1 \leqq a \leqq t} \rho_X{}^*(v_a) \cdot h_a, \text{ where } v_i \in H^*(X).$$

We have $\bar{i}^*w = \sum_{1 \leqq a \leqq s} \bar{i}^*\rho_X{}^*(v_a) \cdot \bar{i}^*h_a$, because $\bar{i}^*h_a = 0$ for $a = s+1, \cdots, t$.

If $\bar{i}^*w = \rho_A{}^*b$, as we have assumed in the lemma we are proving, then

$$\rho_A{}^*b = \sum_{1 \leqq a \leqq s} \rho_A{}^*i^*(v_a) \cdot \bar{i}^*h_a.$$

This is (by uniqueness of the representation) only possible if $i^* v_2 = i^* v_3 = \cdots = i^* v_s = 0$. Thus $\rho_A{}^* b = \rho_A{}^* i^* (v_1)$ $(h_1 = 1)$. Therefore, $b = i^* v_1$, since $\rho_A{}^*$ is a monomorphism. This completes the proof of the lemma.

Proof of (b). By naturality, it is sufficient to prove that the relation $\rho_R{}^*(W_R{}^{q+1}) = S_R{}^{q+1}(x_1, \cdots, x_n)$, $q \geqq r$, holds for the bundle

$$(B_{\boldsymbol{Q}(n)}, \rho(\boldsymbol{Q}(n), \boldsymbol{O}(n)), B_{\boldsymbol{O}(n)}, \boldsymbol{F}(n), \boldsymbol{O}(n)),$$

where ρ_R is written for $\rho_R(\boldsymbol{Q}(n), \boldsymbol{O}(n))$. This is easily seen using the fact that the map $f\colon K \to B_{\boldsymbol{O}(n)}$ inducing the given $\boldsymbol{O}(n)$-bundle over K may be approached by a *simplicial injective* map g as soon as $\dim B_{\boldsymbol{O}(n)} \geqq 2 \cdot \dim K + 1$ (for the existence of g, see Theorem 5 in S. Eilenberg, On spherical cycles, Bulletin of the American Mathematical Society, vol. 47 (1941), pp. 432-434).

Let $(B_{\boldsymbol{O}(r)}, \rho_{r,n}, B_{\boldsymbol{O}(n)}, V_{n,n-r}, \boldsymbol{O}(n))$ be the bundle associated to the classifying bundle for $\boldsymbol{O}(n)$, with fibre $V_{n,n-r}$. The bundle space of this bundle is classifying space for $\boldsymbol{O}(r)$ and is consequently denoted by $B_{\boldsymbol{O}(r)}$. The projection $\rho_{r,n}$ is the Borel map $\rho(\boldsymbol{O}(r), \boldsymbol{O}(n))$.

Consider the following commutative diagram

(5.4)
$$\begin{tikzcd}
B_{\boldsymbol{Q}(r)} \arrow[r, "\mu"] \arrow[d, "\mu^1"'] & B_{\boldsymbol{Q}(n)} \arrow[d] \\
B_{\boldsymbol{O}(r)} \arrow[r, "\rho_{r,n}"] & B_{\boldsymbol{O}(n)}
\end{tikzcd}$$

and let A be a closed subset of $B_{\boldsymbol{O}(n)}$, such that a cross-section θ^r over A is given in the bundle $(B_{\boldsymbol{O}(r)}, \rho_{r,n}, B_{\boldsymbol{O}(n)}, V_{n,n-r}, \boldsymbol{O}(n))$. Let $\bar{A}$ be defined as at the beginning of this section. As noticed previously, $\bar{A}$ is homeomorphic to a subset $\bar{A}^1$ of $B_{\boldsymbol{Q}(r)}$ and $\mu(\bar{A}^1) = \bar{A}$. We have to prove that the element $y = \rho_R{}^*(W_R{}^{q+1}) - S_R{}^{q+1}(x_1, \cdots, x_n) \in H^*(B_{\boldsymbol{Q}(n)}, \bar{A})$ is zero.

Let us consider the following commutative diagram

$$\begin{tikzcd}
\cdots \arrow[r] & H^q(B_{\boldsymbol{Q}(r)}) \arrow[r, "\bar{i}^*"] & H^q(\bar{A}^1) \arrow[r, "\delta"] & H^{q+1}(B_{\boldsymbol{Q}(r)}, \bar{A}^1) \arrow[r] & H^{q+1}(B_{\boldsymbol{Q}(r)}) \arrow[r] & \cdots \\
\cdots \arrow[r] & H^q(B_{\boldsymbol{Q}(n)}) \arrow[r, "i^*"] \arrow[u, "\mu^*"'] & H^q(\bar{A}) \arrow[r, "\delta"] \arrow[u, "\mu_A{}^*"'] & H^{q+1}(B_{\boldsymbol{Q}(n)}, \bar{A}) \arrow[r, "a^*"] \arrow[u, "\mu_R{}^*"'] & H^{q+1}(B_{\boldsymbol{Q}(n)}) \arrow[r] \arrow[u, "\mu^*"'] & \cdots
\end{tikzcd}$$

in which the rows are the cohomology sequences of the pairs $(B_{\boldsymbol{Q}(r)}, \bar{A}^1)$ and $(B_{\boldsymbol{Q}(n)}, \bar{A})$ respectively.

In order to prove $y=0$, it is sufficient to prove $\mu_R^*(y)=0$ and $a^*(y)=0$. Indeed, if these two equalities hold, there exist elements $z\in H^q(\bar{A})$ and $t\in H^q(B_{Q(r)})$, such that $\bar{i}^*t=\mu_A{}^*z$ and $\delta z=y$. Now,

$$H^*(B_{Q(n)};\mathbf{Z}_2)=\mathbf{Z}_2[x_1,\cdots,x_n],H^*(B_{Q(r)};\mathbf{Z}_2)=\mathbf{Z}_2[y_1,\cdots,y_r]$$

and $\mu^*x_i=y_i$ for $i=1,2,\cdots,r$, $\mu^*x_{r+j}=0$ for $j=1,\cdots,n-r$. Thus, μ^* is an epimorphism in every dimension. Therefore, there exists an element $w\in H^q(B_{Q(n)})$, such that $\mu^*w=t$. It follows that $y=\delta z=\delta\mu_A{}^{*-1}\bar{i}^*\mu^*w=\delta i^*w=0$.

It remains to prove that $\mu_R{}^*y=0$ and $a^*y=0$.

Proof of $a^*y=0$. This is obvious with regard to the corresponding result of Borel on absolute characteristic classes:

$$a^*y=a^*\rho_R{}^*W_R{}^{q+1}-a^*S_R{}^{q+1}(x_1,\cdots,x_n)=\rho^*W^{q+1}-S^{q+1}(x_1,\cdots,x_n)=0$$

Proof of $\mu_R{}^*y=0$. We prove separately that $\mu_R{}^*\rho_R{}^*W_R{}^{q+1}=0$ and $\mu_R{}^*S_R{}^{q+1}(x_1,\cdots,x_n)=0$.

The first assertion follows from $\mu_R{}^*\rho_R{}^*W_R{}^{q+1}=\mu_1{}^*\rho_{r,n}{}^*W_R{}^{q+1}$ (see diagram (5.4)), and $\rho_{r,n}{}^*W_R{}^{q+1}=0$ proved in Lemma (5.2).

The second assertion, $\mu_R{}^*S_R{}^{q+1}(x_1,\cdots,x_n)=0$ follows from $\mu^*x_{r+j}=0$ for $j=1,2,\cdots,n-r$ (and thus $\mu_R{}^*x_{r+j}=0$, since $a^*\colon H^1(B_{Q(r)},\bar{A}^1)\to H^1(B_{Q(r)})$ is a monomorphism, A being assumed to be non-void) and the fact that for $q\geqq r$, each product of $(q+1)$ distinct factors from $x_1,\cdots,x_n$ must contain at least one x_{r+j} with $1\leqq j\leqq n-r$. Thus each product in $S_R{}^{q+1}(x_1,\cdots,x_n)$ is mapped into zero by $\mu_R{}^*$.

This completes the proof of Theorem (5.1).

6. A lemma on Lefschetz-Poincaré duality.

Let $\boldsymbol{G}_1$, $\boldsymbol{G}_2$, $\boldsymbol{G}$ be coefficient groups (abelian) with a pairing $\boldsymbol{G}_1\times\boldsymbol{G}_2\to\boldsymbol{G}$ of the two first groups to the third.

Let (X,A) be an admissible pair for cohomology theory. Assume X to be connected and A to be a neighborhood retract in X (hence the excision $e\colon(X,A)\to(Y,X')$ induces an isomorphism $H^*(Y,X')\to H^*(X,A)$).

Let Y be the space obtained by matching together two copies of X along the copies of A (i.e., $Y=X+X'$, with A and A' pointwise identified).

Let n be some positive integer. Denote by ${}_1H$, ${}_2H$, H cohomology groups with coefficients in $\boldsymbol{G}_1$, $\boldsymbol{G}_2$, $\boldsymbol{G}$ respectively.

LEMMA (6.1). *Assume* $H^n(X)=0$, *then the pairings of* ${}_1H^q(X)$ *with* ${}_2H^{n-q}(X,A)$ *to* $H^n(X,A)$ *and of* ${}_1H^q(X,A)$ *with* ${}_2H^{n-q}(X)$ *to* $H^n(X,A)$

given by the cup-product are completely orthogonal if and only if the pairing of ${}_1H^q(Y)$ *with* ${}_2H^{n-q}(Y)$ *to* $H^n(Y)$ *is completely orthogonal* (q, n fixed, $0 \leqq q \leqq n$).

Recall that a pairing is said to be completely orthogonal if either of the first two groups involved is the group of all homomorphisms of the other into the third.

Proof. Consider for $a = 1, 2$ the cohomology sequence of the pair (Y, X)

$$\cdots \to {}_aH^{q-1}(X) \xrightarrow{\delta} {}_aH^q(Y, X) \xrightarrow{h^*} {}_aH^q(Y) \xrightarrow{i^*} {}_aH^q(X) \to \cdots.$$

Since (by excision) the inclusion map $e \colon (X', A') \to (Y, X)$ induces isomorphisms $e^* \colon {}_aH^q(Y, X) \to {}_aH^q(X', A')$, we may substitute ${}_aH^q(X', A')$ for ${}_aH^q(Y, X)$ in the above sequence. Specifically, we consider the exact sequence

$$\cdots \to {}_aH^{q-1}(X) \xrightarrow{\delta'} {}_aH^q(X', A') \xrightarrow{j'^*} {}_aH^q(Y) \xrightarrow{i^*} {}_aH^q(X) \to \cdots,$$

where $\delta' = e^*\delta$ and $j'^* = h^* e^{*-1}$.

Let $k \colon Y \to X$ be the map defined by $k(x) = x$, $k(x') = x$, where x' corresponds to x in the copy X' of X. One has $ki = \text{id.}$, and therefore $i^*k^* = \text{id.}$. Thus i^* is an epimorphism, k^* a monomorphism and δ' is trivial. The sequence

$$0 \to {}_aH^q(X', A') \xrightarrow{j'^*} {}_aH^q(Y) \xrightarrow{i^*} {}_aH^q(X) \to 0$$

is exact.

Moreover, ${}_aH^q(Y)$ is the direct sum

$$(6.2) \qquad {}_aH^q(Y) = j'({}_aH^q(X', A')) + k({}_aH^q(X))$$

(we drop the stars by j'^* and k^* for notational convenience), or alternatively, interchanging X and X':

$$(6.3) \qquad {}_aH^{n-q}(Y) = k'({}_aH^{n-q}(X')) + j({}_aH^{n-q}(X, A)).$$

Let us denote by $l' \colon {}_aH^q(Y) \to {}_aH^q(X', A')$, respectively $l \colon {}_aH^q(Y) \to {}_aH^q(X, A)$ the homomorphisms, such that $l'j' = \mathit{id.}$, and $lj = \mathit{id.}$.

We have, for every $u_1 \in {}_1H^q(Y)$ and $x \in {}_2H^{n-q}(X, A)$,

$$(6.4) \qquad j(iu_1 \cdot x) = u_1 \cdot jx,$$

which may be proved using 3.4 of [11]. Setting $u_1 = ka$ and $x = ly$, one obtains

$$l(ka \cdot y) = a \cdot ly. \tag{6.5}$$

Similarly,

$$l'(b \cdot k'x') = l'b \cdot x'. \tag{6.5'}$$

1. *Assume the pairings of* ${}_1H^q(X)$ *with* ${}_2H^{n-q}(X, A)$ to $H^n(X, A)$ *and of* ${}_1H^q(X, A)$ *with* ${}_2H^{n-q}(X)$ *to* $H^n(X, A)$ *to be completely orthogonal.*

(1a) Let $h\colon {}_2H^{n-q}(Y) \to H^n(Y)$ be a homomorphism. Define the homomorphisms $g\colon {}_2H^{n-q}(X, A) \to H^n(X, A)$ and $g'\colon {}_2H^{n-q}(X') \to H^n(X', A')$ by $g(x) = lhjx$ and $g'(x') = l'hk'x'$ respectively. By assumption, there exist elements $a \in {}_1H^q(X)$ and $a' \in {}_1H^q(X', A')$, such that $g(x) = a \cdot x$ and $g'(x') = a' \cdot x'$ for every $x \in {}_2H^{n-q}(X, A)$ and $x' \in {}_2H^{n-q}(X')$. Set $b = ka + j'a'$ (thus $ib = a$, $l'b = a'$). We have $h(y) = b \cdot y$ for every $y \in {}_2H^{n-q}(Y)$. Indeed, each y admits a decomposition $y = k'x' + jx$ and $lhjx = g(x) = a \cdot x$, $l'hk'x' = g'(x') = a' \cdot x'$.

Therefore, $h(y) = hjx + hk'x' = j(a \cdot x) + j'(a' \cdot x')$. Notice that

$$l'(b \cdot k'x') = l'b \cdot x' = a' \cdot x'$$

(by (6.5')). We obtain

$$h(y) = j(ib \cdot x) + j'l'(b \cdot k'x') = b \cdot jx + b \cdot k'x' = b \cdot (jx + k'x') = b \cdot y$$

($j'l' = \text{id.}$ in dimension n follows from $H^n(X) = 0$, because then $l'\colon H^n(Y) \to H^n(X', A')$ is an isomorphism).

(1b) Suppose that $b \cdot y = 0$ for some $b \in {}_1H^q(Y)$ and every $y \in {}_2H^{n-q}(Y)$. We have to prove $b = 0$. By (6.2), b admits a decomposition $b = j'a' + ka$. We have $j(a \cdot x) = j(ib \cdot x) = b \cdot jx = 0$, furthermore, $a' \cdot x' = l'(b \cdot k'x') = l'(0) = 0$ for every $x \in {}_2H^{n-q}(X, A)$ and $x' \in {}_2H^{n-q}(X')$. By assumption, it follows that $a = a' = 0$. Thus, $b = 0$.

(1a) and (1b) prove that the pairing of ${}_1H^q(Y)$ with ${}_2H^{n-q}(Y)$ to $H^n(Y)$ is completely orthogonal.

2. *Assume now the pairing of* ${}_1H^q(Y)$ *with* ${}_2H^{n-q}(Y)$ *to* $H^n(Y)$ *to be completely orthogonal.*

(2a) Take a homomorphism $h\colon {}_2H^{n-q}(X, A) \to H^n(X, A)$. By (6.3), each $y \in {}_2H^{n-q}(Y)$ may be written uniquely in the form $y = k'x' + jx$. The map $g\colon {}_2H^{n-q}(Y) \to H^n(Y)$ defined by $g(y) = jh(x)$ is a homomorphism and thus, by assumption, there exists an element $u_1 \in {}_1H^q(Y)$, such that $u_1 \cdot y = jh(x)$ for every $y = k'x' + jx \in {}_2H^{n-q}(Y)$. One has (with $u = iu_1$),

$j(u \cdot x) = j(iu_1 \cdot x) = u_1 \cdot jx = jh(x)$. Since j is a monomorphism, $u \cdot x = h(x)$ for every $x \in {}_2H^{n-q}(X, A)$.

(2b) Let $a \cdot x = 0$ for some $a \in {}_1H^q(X)$ and every $x \in {}_2H^{n-q}(X, A)$. Then $a = 0$. Indeed, consider $ka = b \in {}_1H^q(Y)$. We have $b \cdot y = 0$ for every $y \in {}_2H^{n-q}(Y)$, because $l(b \cdot y) = l(ka \cdot y) = a \cdot ly = 0$. In dimension n, l is a monomorphism, because $H^n(X) = 0$. The pairing of ${}_1H^q(Y)$ with ${}_2H^{n-q}(Y)$ to $H^n(Y)$ being assumed to be completely orthogonal, it follows that $b = 0$. Thus, $a = ika = ib = 0$.

The proofs of (2a′): every homomorphism ${}_2H^{n-q}(X) \to H^n(X, A)$ may be "realized" by cup-product with an element of ${}_1H^q(X, A)$ and of (2b′): if $a \cdot x = 0$ for some $a \in {}_1H^q(X, A)$ and every $x \in {}_2H^{n-q}(X)$, then $a = 0$, are mechanical and similar to (2a) and (2b) and will be omitted.

Remark. The assumption $H^n(Y) = 0$ is actually needed in the proofs of both (1) and (2) as is shown by the following examples.

(1) Let $X = P_5$ be the 5-dimensional real projective space and A a point of P_5. Let $\boldsymbol{G}_1 = \boldsymbol{G}_2 = \boldsymbol{G} = \boldsymbol{Z}_2$ and take $n = 5$, $q = 2$. Then ${}_1H^2(X) \cong {}_2H^3(X, A) \cong H^5(X, A) \cong \boldsymbol{Z}_2$ and the pairing of ${}_1H^2(X)$ with ${}_2H^3(X, A)$ to $H^5(X, A)$ by cup-product is completely orthogonal. Similarly, the pairing of ${}_1H^2(X, A)$ with ${}_2H^3(X, A)$ is also completely orthogonal.

Now $Y = P_5 \vee P_5$ and ${}_1H^2(Y) \cong {}_2H^3(Y) \cong H^5(Y) \cong \boldsymbol{Z}_2 + \boldsymbol{Z}_2$. However, $\mathrm{Hom}(\boldsymbol{Z}_2 + \boldsymbol{Z}_2, \boldsymbol{Z}_2 + \boldsymbol{Z}_2) \cong \boldsymbol{Z}_2 + \boldsymbol{Z}_2 + \boldsymbol{Z}_2 + \boldsymbol{Z}_2$. One has $H^5(X) \cong \boldsymbol{Z}_2$.

(2) Let $X = A = S_1$. Then $Y = X = S_1$. Take $n = 1$, $q = 0$ and $\boldsymbol{G}_1 = \boldsymbol{G}_2 = \boldsymbol{G} = \boldsymbol{Z}$. The pairing of ${}_1H^0(Y) = \boldsymbol{Z}$ with ${}_2H^1(Y) = \boldsymbol{Z}$ to $H^1(Y) = \boldsymbol{Z}$ is completely orthogonal, but since ${}_2H^1(X, A) = 0$, $H^1(X, A) = 0$, the pairing of ${}_1H^0(X) = \boldsymbol{Z}$ with ${}_2H^1(X, A)$ to $H^1(X, A)$ is not. One has $H^1(X) = \boldsymbol{Z}$.

7. The relative Wu classes.

We come back to coefficients in the field $\boldsymbol{Z}_2$.

Let K be a complex of dimension n and L a non-void subcomplex of K. Suppose that relative Lefschetz-Poincaré duality holds in $K \bmod L$. In other words, for every $q = 0, 1, \cdots, n$, the pairing of $H^q(K; \boldsymbol{Z}_2)$ with $H^{n-q}(K, L; \boldsymbol{Z}_2)$ to $H^n(K, L; \boldsymbol{Z}_2)$ is completely orthogonal. Then we may define Wu classes $U^q \in H^q(K; \boldsymbol{Z}_2)$ by the requirement that for every relative class $X_R^{n-q} \in H^{n-q}(K, L)$

$$Sq^q(X_R^{n-q}) = U^q \cdot X_R^{n-q} \tag{7.1}$$

should hold.

Because L is non-empty, $H^0(K,L)=0$, and thus, by duality, $H^n(K)=0$. Consequently, according to Lemma (6.1), absolute Poincaré duality holds in $M=K+K'$ (L and L' identified). Let S^q be the q-dimensional Wu class of M (in the ordinary sense, see [16]), i.e.,

$$(7.2) \qquad Sq^q(X^{n-q})=S^q\cdot X^{n-q}$$

for every class $X^{n-q}\in H^{n-q}(M)$.

LEMMA (7.3). *Let $i\colon K\to M$ be the inclusion map and i^* the dual homomorphism induced by i, then $U^q=i^*S^q$.*

Proof. Let $j^*\colon H^*(K,L)\to H^*(M)$ be as in (6.3). We have, using (6.4), $j^*(i^*S^q\cdot X_R^{n-q})=S^q\cdot j^*X_R^{n-q}=Sq^q(j^*X_R^{n-q})=j^*(Sq^q(X_R^{n-q}))$. Since j^* is a monomorphism and the class U^q is determined uniquely by (7.1), it follows that $U^q=i^*S^q$.

Suppose now a sphere-bundle is given over M such that its Stiefel-Whitney characteristic classes $W_M{}^q$ be connected to the Wu classes by the relation

$$(7.4) \qquad W_M{}^q=\sum_{0\leqq p\leqq q}Sq^{q-p}(S^p),$$

which we may write more conveniently as $W_M=Sq(S)$, denoting by W_M and S the "total" classes, i.e.,

$$W_M=1+W_M{}^1+\cdots+W_M{}^n, \qquad S=1+S^1+\cdots+S^n$$

and where the operator Sq stands for $Sq=Sq^0+Sq^1+\cdots+Sq^k+\cdots$.

According to a theorem of Wu in [16], the situation described by formula (7.4) arises in particular if M is a closed differentiable manifold and the sphere-bundle considered is its tangent bundle. From the relative Lefschetz-Poincaré duality for manifolds with regular boundary ([11], 7), it follows that (7.4) *holds in particular with $M=K+K'$ if K is a manifold with regular boundary L.*

Since the characteristic classes of the restricted bundle over K are the i^*-images of the characteristic classes of the bundle over M (by naturality), we have $W=Sq(U)$, where W denotes the total Stiefel-Whitney class of the bundle over K.

Suppose now that

(7.5) *a cross-section over the subcomplex L is given in the associated principal bundle.*

Then, for every q, W^q admits a representative cocycle which vanishes on L and thus defines a relative class $W_R{}^q$.

Since $H^0(K,L)=0$, the algebra $H^*(K,L)$ has no unit element. It is convenient to consider, rather than $H^*(K,L)$, the direct sum $H_1^*=\mathbf{Z}_2+H^*(K,L)$. In other words, we introduce formally a unit into the algebra $H^*(K,L)$. The requirement $1\cdot x=x\cdot 1=x$ for every $x\in H_1^*$ gives to H_1^* a ring structure. We shall furthermore allow the Steenrod squares to operate (as homomorphisms again) in H_1^* by setting $Sq^0(1)=1$, $Sq^i(1)=0$ for $i>0$.

We may then use the classes W_R^q to define a total relative class by $W_R=1+W_R^1+\cdots+W_R^n\in H_1^*$. Since the endomorphism $Sq\colon H_1^*\to H_1^*$ defined for each $X\in H_1$ by $Sq(X)=Sq^0(X)+Sq^1(X)+\cdots$ is a monomorphism and therefore maps H_1^*, as a finite dimensional vector space, *onto* itself, we may define *relative Wu classes* U_R^q by

$$W_R=Sq(U_R), \tag{7.6}$$

U_R being the total class $U_R=1+U_R^1+U_R^2+\cdots\in H_1^*$.

Notice furthermore, that according to the above conventions, we have $Sq(1)=1$, and therefore the product formula of H. Cartan

$$Sq(X\cdot Y)=Sq(X)\cdot Sq(Y) \tag{7.7}$$

holds also in H_1^*.

We state now some properties of the relative Wu class U_R.

LEMMA (7.8). *Let h: $(K,0)\to(K,L)$ be the inclusion map and h^* the induced homomorphism, then $U^q=h^*U_R^q$ for every $q>0$.*

The proof is immediate: Apply h^* to both sides of the equation (7.6) $W_R=Sq(U_R)$, with the convention $h^*(1)=1$. We obtain $W=Sq(h^*U_R)$. Since the class U is uniquely determined by $W=Sq(U)$, Sq being an automorphism of $H^*(K)$, it follows that $U=h^*U_R$.

LEMMA (7.9). *For every relative class $X_R^{n-q}\in H^{n-q}(K,L)$, we have $Sq^q(X_R^{n-q})=U_R^q\cdot X_R^{n-q}$.*

This is again obvious, according to the preceding lemma.

The following is a discrepancy between properties of absolute and relative Wu classes: Absolute classes the dimension of which exceed $\frac{1}{2}n$ vanish (if $q>\frac{1}{2}n$, then $q>n-q$; thus, in formula (7.1), the square is zero for every X_R^{n-q} and, by duality U^q, must be zero, too). This need *not* be the case for relative Wu classes.

We shall be mainly interested in the sequel in the case *n even.* We state some lemmas in this case:

LEMMA (7.10). *Let n be even, $n = 2s$. Under assumptions* (7.4) *and* (7.5), *we have* $W_R{}^n = U_R{}^s \cdot U_R{}^s + U_R{}^{2s}$.

Proof.

$$\begin{aligned} W_R{}^n &= Sq^s(U_R{}^s) + Sq^{s-1}(U_R{}^{s+1}) + \cdots + Sp^{s-i}(U_R{}^{s+i}) + \cdots + U_R{}^{2s} \\ &= U_R{}^s \cdot U_R{}^s + U_R{}^{s-1} \cdot U_R{}^{s+1} + \cdots + U_R{}^{s-i} \cdot U_R{}^{s+i} + \cdots + U_R{}^{2s} \\ &= U_R{}^s \cdot U_R{}^s + Sq^{s+1}(U_R{}^{s-1}) + \cdots + Sq^{s+i}(U_R{}^{s-i}) + \cdots + U_R{}^{2s} \\ &= U_R{}^s \cdot U_R{}^s + U_R{}^{2s}. \end{aligned}$$

LEMMA (7.11). *Suppose K has even dimension $n = 2s$. Let r be the rank of the bilinear form $f(X, Y)$ over $\mathbf{Z}_2$ defined for $X, Y \in H^s(K, L; \mathbf{Z}_2)$ by $X \cdot Y = f(X, Y)A$, where A denotes the generator of $H^n(K, L)$. Then, under assumptions* (7.4) *and* (7.5) $r \cdot A = U_R{}^s \cdot U_R{}^s$.

Proof. Introduce in $H^s(K, L)$ a basis $Z_1, \cdots, Z_r, Z_{r+1}, \cdots, Z_p$, such that $Z_i \cdot Z_j = \delta_{ij} A$ for $1 \leqq i, j \leqq r$ and $Z_i \cdot Z_j = 0$ if $r < i$ or $r < j$.

With respect to such a basis, $U_R{}^s$ must have the form

$$U_R{}^s = Z_1 + Z_2 + \cdots + Z_r + c_{r+1} Z_{r+1} + \cdots + c_p Z_p.$$

Indeed, let $U_R{}^s = \sum_{1 \leqq i \leqq p} c_i Z_i$, with $c_i \in \mathbf{Z}_2$, and let $X = \sum_{1 \leqq i \leqq p} x_i Z_i$ be any class in $H^s(K, L)$. One has

$$Sq^s(X) = X \cdot X = x_1{}^2 + x_2{}^2 + \cdots + x_r{}^2 = x_1 + x_2 + \cdots + x_r \pmod 2,$$

$$U_R{}^s \cdot X = c_1 x_1 + c_2 x_2 + \cdots + c_r x_r.$$

Thus, for any choice of $x_1, \cdots, x_r$, Lemma (7.9) implies

$$x_1 + x_2 + \cdots + x_r = c_1 x_1 + c_2 x_2 + \cdots + c_r x_r.$$

This is only possible if $c_1 = c_2 = \cdots = c_r = 1$.

Now from $U_R{}^s = Z_1 + Z_2 + \cdots + Z_r + c_{r+1} Z_{r+1} + \cdots + c_p Z_p$, it follows that $U_R{}^s \cdot U_R{}^s = Z_1 \cdot Z_1 + Z_2 \cdot Z_2 + \cdots + Z_r \cdot Z_r = rA$, and the proof of (7.11) is complete.

We consider now the dual classes $\bar{W}_R$ and $\bar{U}_R$ which are defined by

$$(7.12) \qquad W_R \cdot \bar{W}_R = 1, \qquad U_R \cdot \bar{U}_R = 1$$

respectively. $\bar{W}_R$ and $\bar{U}_R$ are uniquely defined (as relative classes) because the cup-product with a total class U_R or W_R defines an *isomorphism* $H_1{}^* \to H_1{}^*$

of $H_1{}^*$ onto itself. Of course, $\bar{W} = h^*\bar{W}_R$ and similarly with U substituted for W.

We have

$$\bar{W}_R = Sq(\bar{U}_R). \tag{7.13}$$

Proof. Denoting $Sq(\bar{U}_R)$ by $\tilde{\bar{W}}_R = Sq(\bar{U}_R)$, we have

$$W_R \cdot \tilde{\bar{W}}_R = Sq(U_R) \cdot Sq(\bar{U}_R) = Sq(U_R \cdot \bar{U}_R) = Sq(1) = 1.$$

Since $W_R \cdot \bar{W}_R = 1$ determines $\bar{W}_R$ uniquely, $\tilde{\bar{W}}_R = \bar{W}_R$.

Lemma (7.14). *We have (with $n = 2s$ and under assumptions* (7.4), (7.5)) $rA^n = W^{n-1} \cdot \bar{W}_R{}^1 + W^{n-2} \cdot \bar{W}_R{}^2 + \cdots + W^1 \cdot \bar{W}_R{}^{n-1}$, *where* $W^q = h^*W_R{}^q$ *as in* (7.8); r *and* A^n *were defined in* (7.11).

Proof. We prove first $\bar{W}_R{}^n = U_R{}^n$, as follows:

$$\begin{aligned}
\bar{W}_R{}^n &= Sq^0(\bar{U}_R{}^n) + Sq^1(\bar{U}_R{}^{n-1}) + \cdots + Sq^s(\bar{U}_R{}^s) \\
&= \bar{U}_R{}^n + U_R{}^1 \cdot \bar{U}_R{}^{n-1} + \cdots + U_R{}^s \cdot \bar{U}_R{}^s \\
&= U_R{}^{s+1} \cdot \bar{U}_R{}^{s-1} + \cdots + U_R{}^{n-1} \cdot \bar{U}_R{}^1 + U_R{}^n \quad \text{(by (7.12))} \\
&= Sq^{s+1}(\bar{U}_R{}^{s-1}) + \cdots + Sq^{n-1}(\bar{U}_R\ ) + U_R{}^n = U_R{}^n.
\end{aligned}$$

From $W_R{}^n + W_R{}^{n-1} \cdot \bar{W}_R{}^1 + \cdots + W_R{}^1 \cdot \bar{W}_R{}^{n-1} + \bar{W}_R{}^n = 0$, we obtain

$$W_R{}^n = W_R{}^{n-1} \cdot \bar{W}_R{}^1 + \cdots + W_R{}^1 \cdot \bar{W}_R{}^{n-1} + U_R{}^n.$$

Comparing this formula with (7.10) and (7.11), we see that

$$rA^n = W_R{}^{n-1} \cdot \bar{W}_R{}^1 + \cdots + W_R{}^1 \cdot \bar{W}_R{}^{n-1},$$

hence $rA^n = W^{n-1} \cdot \bar{W}_R{}^1 + \cdots + W^1 \cdot \bar{W}_R{}^{n-1}$. This completes the proof of Lemma (7.14).

PART II. Proof and Consequences of Lemma (1.2).

8. The proof. All homology and cohomology groups occurring in this section will be based on remainders mod 2 as coefficients (we shall therefore omit to mention the coefficient field explicitly).

Consider the situation described in Section 1: a C^∞-d-manifold M_d regularly imbedded in euclidean $(d+n)$-space E_{d+n} with a continuous field of normal n-frames $\boldsymbol{F}_n$. In order to prove the Lemma (1.2), i.e., $\gamma = h$, it is sufficient to consider the special case $n = d+1$. Indeed, if $\gamma(f) = h(f)$ has been proved for every $f \in \pi_{2d+1}(S_{d+1})$, the general assertion follows from the fact that γ and h are both "stable" by suspension (Section 1, property (3)): If $f \in \pi_{d+n}(S_n)$, with $n \leqq d+1$, then $\gamma(f) = \gamma(E^{d+1-n}f) = h(E^{d+1-n}f) = h(f)$. If $f \in \pi_{d+n}(S_n)$, with $n \geqq d+1$, then there exists by Freudenthal's theorems a map $g \in \pi_{2d+1}(S_{d+1})$, such that $E^{n-d-1}g = f$, and for the same reason $\gamma(f) = \gamma(g) = h(g) = h(f)$.

In the sequel $n = d+1$. Let $f\colon S_{2d+1} \rightarrow S_{d+1}$ be the sphere map corresponding to the given manifold M_d in E_{2d+1}, together with the n-field $\boldsymbol{F}_n$ ($n = d+1$) of mutually orthogonal unit vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_n$ normal to M_d in E_{d+n} (see Section 1, (b)). It is easily seen from the definition of f (see (1.1)) that $M_d = f^{-1}(q)$, where q is the point of S_n with the coordinates $q = (1, 0, \cdots, 0)$. Furthermore, the manifold M'_d, which is the locus of the endpoint of the vector $\epsilon\boldsymbol{v}_1(x)$ as x runs over M_d (ϵ fixed, a small positive real number) is also the reverse image $M'_d = f^{-1}(q')$ of some point $q' \in S_n$ (precisely, q' is the point $q' = (1-2\epsilon^2, 2\epsilon(1-\epsilon^2)^{\frac{1}{2}}, 0, \cdots, 0)$, if the mapping $r\colon B_n \rightarrow S_n$ is indeed chosen as in (1.1)).

By the original definition of Hopf's invariant, one has

$$L(M_d, M'_d) = h(f) \mod 2, \tag{8.1}$$

where $L(\ ,\ )$ denotes the looping coefficient in E_{2d+1}.

Considering E_{2n-1} ($= E_{2d+1}$) as the linear subspace of E_{2n} defined by $y_{2n} = 0$, $y_1, y_2, \cdots, y_{2n-1}$ being coordinates in E_{2n-1}, we show first that there exists in E_{2n} an immersed (not necessarily orientable) manifold X_n, the regular boundary (mod 2) of which is the given manifold M_d imbedded in E_{2n-1}.

The existence of an abstract C^∞-manifold V_n with regular boundary (mod 2) diffeomorphic to M_d follows, by a theorem of R. Thom (see [14], Théorème IV. 10), from the fact that all Stiefel-Whitney numbers of M_d vanish mod 2 (this because the normal bundle over M_d is trivial). We want to prove the existence of an immersion $i\colon V_n \rightarrow E_{2n}$, such that $i|\partial V_n$ be the given imbedding $f\colon M_d \rightarrow E_{2n-1}$.

By Theorem 1 in Whitney's paper [15], there exists an analytic manifold A_n in euclidean $(2n+1)$-space E, which is C^2-homeomorphic to V_n. Map A_n into E_{2n} by F_0 defined as follows: $F_0|\partial A_n$ is the given imbedding f of $M = \partial A_n$ into E_{2n-1}. Consider a neighborhood $N \approx \partial A_n \times I$ of ∂A_n in A_n and represent points $u \in N$ by pairs (x, t), where $x \in \partial A_n$ and $0 \leqq t \leqq 1$. Define $F_0(u) = (fx, t) =$ the point of E_{2n} with $(2n-1)$ first coordinates coinciding with those of fx and the $2n$-th coordinate of which is t. Extend F_0 over A_n, such that $F_0(A - N) \subset \{y_{2n} > 1\}$. Let N_1 be the subset of N characterized by $0 \leqq t \leqq \frac{1}{3}$. Extending again F_0 over E now, we use Weierstrass' approximation theorem to get a C^2 map $F_1\colon A_n \to E_{2n}$, such that $F_1(\overline{A - N_1}) \cap E_{2n-1} = 0$. Let ω^0 be a real valued C^2 function on A_n, such that $\omega^0 = 1$ in $A - N$, $\omega^0 = 1$ in N for $t \geqq \frac{2}{3}$, $0 \leqq \omega^0 \leqq 1$ for $\frac{1}{3} \leqq t \leqq \frac{2}{3}$, $\omega^0 = 0$ for $t \leqq \frac{1}{3}$. Take, for instance, $\omega^0(x,t) = \frac{1}{4}(1 + \cos(3\pi t))^2$ for (x,t) in N with $\frac{1}{3} \leqq t \leqq \frac{2}{3}$. For $u \in N$, $F_1(u)$ has the form $F_1(u) = F_0(u) + \xi(u)$. Define $F\colon A_n \to E_{2n}$ by $F | A - N = F_1 | A - N$ and $F(u) = F_0(u) + \omega^0(u)\xi(u)$. Then F is C^2 and its restriction over ∂A_n is f. Moreover, $F | N_1 = F_0 | N_1$, and thus F is completely regular in N_1 since F_0 is.

Now, by a theorem of H. Whitney (see [15], Theorem 2, assertions (a) and (b)), we can approximate F, together with its first derivatives by a completely regular immersion $j\colon A_n \to E_{\;n}$. Let N_2 be the subset of N_1 defined by $0 \leqq t \leqq \frac{1}{9}$ and define the C^2 real-valued function ω^1 over A_n by $\omega^1(x) = 1$ for $x \in A - N_1$, $\omega^1(u) = 1$ for $\frac{2}{9} \leqq t \leqq \frac{1}{3}$, $\omega^1(u) = \frac{1}{4} \cdot (1 + \cos(9\pi t))^2$ for $\frac{1}{9} \leqq t \leqq \frac{2}{9}$ and $\omega^1(u) = 0$ for $u \in N_2$. Substitute for j the immersion $i\colon A_n \to E_{2n}$ defined by $i | A - N_1 = j | A - N_1$. In N_1, j takes the form $j(u) = F(u) + \eta(u)$. Define $i(u)$ by $i(u) = F(u) + \omega^1(u)\eta(u)$. Since we may take $\eta(u)$ together with its first derivatives arbitrarily small and the derivatives of $\omega^1(u)$ are all zero except the derivative with respect to t which is $\leqq 20$, it follows that, for suitably chosen j, the map i will be completely regular ($F | N_1 = F_0 | N_1$ is completely regular). Moreover, $i | N_2 = F_0 | N_2$, and therefore *the normal vector to* M_d *and tangent to* $i(A_n)$ *is the constant vector* $\boldsymbol{v}_0$, *normal to* E_{2n-1} *in* E_{2n}. Finally, we can obviously manage that $i(A - \partial A)$ has no common point with E_{2n-1}. Denote $i(A_n)$ by X_n.

We replace now the given field $\boldsymbol{F}_n$ of n-frames $\boldsymbol{v}_1(x), \cdots, \boldsymbol{v}_n(x)$ normal to M_d in E_{2n-1} by the $(n+1)$-field $\boldsymbol{F}_{n+1}$ of $(n+1)$-frames $\boldsymbol{v}_0(x), \boldsymbol{v}_1(x), \cdots, \boldsymbol{v}_n(x)$ consisting of the (constant) vector $\boldsymbol{v}_0(x)$ tangent to X_n and normal to M_d at $x \in M_d$, followed by the vectors of the field $\boldsymbol{F}_n$.

The homotopy class of the map $\omega'\colon M_d \to V_{2n,n+1}$ induced by the $(n+1)$-field $\boldsymbol{F}_{n+1}$ is represented by the same remainder mod 2, i. e., c, as the homotopy class of the map $\omega\colon M_d \to V_{2n-1,n}$ induced by the given field $\boldsymbol{F}_n$ (*we have assumed* d *odd*, which is no loss of generality in view of $\gamma = h = 0$ for d even by [8], Théorème IV. *Thus* $n = d + 1$ *is even*, $n = 2s$).

On the other hand, using certain vectors of $\boldsymbol{F}_{n+1}$ as a cross-section over $M_d \subset X_n$, we can define relative characteristic Stiefel-Whitney classes as follows: the n last vectors of $\boldsymbol{F}_{n+1}$ provide a cross-section over M_d in the principal normal bundle over X_n and lead in every positive dimension to a class $\bar{W}_R{}^i \bmod M_d$ $(1 \leqq i \leqq n)$. The vector field v_0 leads to the characteristic class $W_R{}^n$ of the tangent bundle to X_n. Using finally the vectors of $\boldsymbol{F}_{n+1}$ altogether, we can define the relative n-dimensional class $S_R{}^n$ of the Whitney sum: tangent $\oplus$ normal bundles over X_n. According to Whitney duality for relative characteristic classes (Theorem (4.1)), we have[6]

$$S_R{}^n = W_R{}^n + W^{n-1} \cdot \bar{W}_R{}^1 + \cdots + W^1 \cdot \bar{W}_R{}^{n-1} + \bar{W}_R{}^n. \tag{8.2}$$

The remaining part of the proof of Lemma (1.2) consists in interpreting the several terms occurring in formula (8.2).

First,

$$S_R{}^n = c \cdot A_R{}^n, \tag{8.3}$$

where $A_R{}^n$ denotes the generator of $H^n(X, M; \boldsymbol{Z}_2)$. The class $S_R{}^n$ is indeed the obstruction class to the extension of $\boldsymbol{F}_{n+1}$ over X_n under the only condition that it keeps being an $(n+1)$-framefield in E_{2n}. The formula (8.3) follows then from the fact that $V_{2n,n+1}$ is $(n-2)$-connected.

Since $W_R{}^n$ is the obstruction cohomology class to the extension of the vector $\boldsymbol{v}_0(x)$ as a *tangent* vector field over X, we have by [2] (Satz I, page 549)

$$W_R{}^n = \chi(X) \cdot A_R{}^n. \tag{8.4}$$

It has been proved in Lemma (7.14) that

$$rA_R{}^n = W^{n-1} \cdot \bar{W}_R{}^1 + \cdots + W^1 \cdot \bar{W}_R{}^{n-1}. \tag{8.5}$$

Let us prove now that

$$\bar{W}_R{}^n = h(f) A_R{}^n. \tag{8.6}$$

Indeed, $\bar{W}_R{}^n$ is the obstruction class to the extension over X_n of the vector $\boldsymbol{v}_1(x)$ of the field $\boldsymbol{F}_{n+1}$ as a *unit* vector field *normal* to X_n in E_{2n}. The extension is possible over the $(n-1)$-skeleton (a triangulation of X is taken, such that M is a subcomplex). Suppose this extension has been constructed. Extend then $\boldsymbol{v}_1(x)$ in the interior of the n-simplexes of X_n as a *normal* vector of length $\leqq 1$. This is always possible if we allow $v_1(x)$ to have length 0 in some interior points of some n-simplexes of X_n. Consider the locus X' of the endpoint of the vector $\epsilon v_1(x)$ so extended (where $\epsilon > 0$ is smaller than the radius of a tubular neighborhood of X_n in E_{2n}; see [14], page 27). Denote by $V = X + \bar{X}$ the closed manifold obtained by adding to X its mirror image $\bar{X}$ with respect to the hyperplane E_{2n-1} in E_{2n}. We may choose the extension $v_1(x)$, $x \in X_n$, such that X' and V are in general position in E_{2n}, so that we may determine the intersection coefficient mod 2 of V and X' by simply counting the intersection points. We assume all intersection points to be simple. We have then two kinds of intersection points of X' with V: Those arising from the impossibility of extending $v_1(x)$ in the interior of an n-simplex of X_n as a normal unit vector (let their number be I), and those which arise from self-intersection points of X. It is clear that intersection points of the last category can occur only in *pairs*, thus their number is $2N$, where N is some integer.

---

[6] Notice that we could prove (8.2) as follows: The restriction over M of the normal principal bundle $\mathfrak{N}$ over X is trivial. Let $K = X \cup C$ be obtained by attaching to X the cone over M. Then $\mathfrak{N}$ can be extended over K (i.e., the map $N: X \rightarrow B_{SO(n)}$ inducing $\mathfrak{N}$ can be extended to a map $K \rightarrow B_{SO(n)}$). K being realized in E_{2n}, define $T: K \rightarrow B_{SO(n)}$ by $T(x) = n$-plane orthogonal to $N(x)$ for every $x \in K$. This defines a bundle $\mathfrak{T}$ over K. Let w be the total Stiefel-Whitney class of $\mathfrak{T}$, $\bar{w}$ the total class of $\mathfrak{N}$. By excision, one has $H^+(K) \cong H^+(K, C) \cong H^+(X, M)$, where H^+ is the ring consisting of the elements of positive dimensions in the cohomology ring. It is not difficult to see that these isomorphisms send w^n into $S_R{}^n + W_R{}^n$ and w^i, $\bar{w}^j$ for $1 \leqq i \leqq n$, $1 \leqq j \leqq n$, into $W_R{}^i$, $\bar{W}_R{}^j$ respectively. Ordinary Whitney duality $w \cdot \bar{w} = 0$ goes thus over into formula (8.2) in particular. However, this raisonning does not apply in the more general situation considered in Part I.

By definition of $\bar{W}_R{}^n$, we have $\bar{W}_R{}^n = I A_R{}^n$ modulo 2. Furthermore, $I = I + 2N = S(V, X') = L'(V, M')$ modulo 2, where $L'(\ ,\ )$ denotes the looping coefficient in E_{2n} and M', as before, the locus of the endpoint of $\epsilon v_1(x)$ as x runs over $M_d (\partial X' = M' \bmod 2)$. Since $V \cap E_{2n-1} = M_d$, we have $L'(V, M') = L(M, M')$, where $L(\ ,\ )$ is again the looping coefficient in E_{2n-1}. Therefore, $I = L(M, M') = h(f) \bmod 2$. In other words, $\bar{W}_R{}^n = h(f) A_R{}^n$.

Using the formulae (8.3), (8.4), (8.5) and (8.6), the formula (8.2) translates into

$$c = \chi(X) + r + h(f) \mod 2. \tag{8.7}$$

It has been proved in [8], that

$$\chi^*(M) = \chi(X) + \rho \mod 2, \tag{8.8}$$

where ρ is the rank of the bilinear form $S(x, y)$ defined by the intersection coefficient in $H_s(X_n; \mathbf{Z}_2)$, $n = 2s$ (i.e. $S(x, y)$ is the intersection coefficient of the classes $x, y \in H_s(X_n; \mathbf{Z}_2)$). It is not difficult to see that $\rho = r$. We prove, however,

$$\chi^*(M) = \chi(X) + r \mod 2 \tag{8.9}$$

more simply by considering the exact cohomology sequence of the pair (X, M), i.e.,

$$\begin{aligned} H^s(X) \xleftarrow{h^*} H^s(X, M) \xleftarrow{\delta} H^{s-1}(M) \leftarrow \cdots - H^0(M) \\ \xleftarrow{i^*} H^0(X) \xleftarrow{h^*} H^0(X, M) \leftarrow 0. \end{aligned}$$

Using the completely orthogonal pairing of $H^s(X)$ with $H^s(X,M)$ to $H^n(X,M)$, it follows from $h^*C\cdot Z = C\cdot Z$, $C, Z \in H^s(X,M)$ that the kernel of h^* in $H^s(X,M)$ consists exactly of those elements C for which $C\cdot Z = 0$ for every $Z \in H^s(X,M)$. Thus, we have $r =$ (rank of $H^s(X,M)$) — (rank kernel h^*). Using the exactness of the above sequence, we obtain

$$r = p_s(X,M) - p_{s-1}(M) + p_{s-1}(X) - p_{s-1}(X,M) + \cdots$$
$$+ (-1)^s p_0(M) + (-1)^{s-1} p_0(X) + (-1)^s p_0(X,M),$$

where $p_q(X,M)$, $p_q(M)$, $p_q(X)$ denote the ranks of $H^q(X,M)$, $H^q(M)$, $H^q(X)$ respectively.

Replacing in this formula $p_q(X,M)$ by $p_{n-q}(X)$ according to relative Lefschetz-Poincaré duality in $X \bmod M$, we obtain

$$r = (-1)^s \chi^*(M) + (-1)^{s-1} \sum_{0\leqq i\leqq s-1} (-1)^i p_i(X) + (-1)^s \sum_{s\leqq i\leqq n} (-1)^i p_i(X).$$

In other words,

$$(8.10)\quad \chi^*(M) = \{\sum_{0\leqq i\leqq s-1} (-1)^i p_i(X) - \sum_{s\leqq i\leqq n} (-1)^i p_i(X)\} + (-1)^s \cdot r,$$

from which formula (8.9) follows by reduction modulo 2.

Now, since by definition $\gamma(f) = c - \chi^*(M)$, formulae (8.7) and (8.9) complete the proof of the Lemma (1.2): $\gamma(f) = h(f)$.

9. Consequences of the Lemma (1.2).

Using the Lemma (1.2) we may improve the generalized Curvatura Integra theorem. We obtain first from $h(f) = 0$ if $n \leqq d$ (because then $Sq^{d+1}(u^n) = 0$) the

THEOREM (9.1). *Let the closed differentiable manifold M_d be regularly imbedded in E_{d+n} with a field of normal n-frames $\mathbf{F}_n$ and $n \leqq d$, then the corresponding curvatura integra c does not depend on the imbedding nor on the n-field and is given by $c = \chi^*(M_d)$.*

Indeed, $c - \chi^*(M) = \gamma(f)$, where f is a map $S_{d+n} \to S_n$ as constructed in Section 1, (b). Since $\gamma(f) = h(f) = 0$ because $n \leqq d$, the theorem follows.

Suppose that the integer d is such that every element in $\pi_{2d+n}(S_{d+1})$ has even (or zero) Hopf's invariant. Then every element in $\pi_{d+n}(S_n)$ with arbitrary n has zero generalized Hopf's invariant h. In this case we may therefore omit the restriction on n in the above theorem and obtain the

THEOREM (9.2). *Let the closed differentiable manifold M_d be regularly imbedded in any euclidean space E_{d+n} with a field of normal n-frames*

F_n; if d is such that there is no element of odd Hopf's invariant in $\pi_{2d+1}(S_{d+1})$, then the curvatura integra c corresponding to the imbedding and to F_n depends in fact only on M_d and is given by $c = \chi^*(M_d)$.

We may replace in this theorem the assumption of an *imbedding* of M_d by the weaker one of an *immersion* (with self-intersections allowed). Indeed, if M_d is immersed in E_{d+n} with a field of normal n-frames F_n defining a curvatura integra c, we may imbed E_{d+n} as a linear subspace in E_{d+N} $(n \leqq N)$, with a field of normal N-frames F_N which consists of the n vectors of F_n followed by $(N-n)$ constant mutually orthogonal unit vectors normal to E_{d+n} in E_{d+N}. The curvatura integra corresponding to the new field F_N is again c and if N has been chosen sufficiently large $(d+1 \leqq N)$, a slight deformation in E_{d+N} of the immersion $M_d \to E_{d+N}$ will provide an *imbedding* of M_d into E_{d+N} with a field of normal N-frames obtained by continuous deformation from F_N (apply Theorem 2, case (c) of H. Whitney's paper [15] to obtain the imbedding and the covering homotopy theorem to obtain the desired field). The curvatura integra c still belongs to the new situation to which now Theorem (9.2) applies (d has not been changed). Thus we obtain the

THEOREM (9.2*). *The thorem (9.2) is still valid replacing the assumption of an "imbedding" of M_d by the assumption of an "immersion."*

Of special interest may be the case $n = 1$, originally considered by Hopf for d even. If d is odd and the manifold M_d assumed to be imbedded in E_{d+1}, then the curvatura integra c (the degree of the Gauss mapping $M_d \to S_d$, in this case) is modulo 2 equal to $\chi^*(M_d)$. This was proved in [8] and also by J. Milnor, using a simpler method especially adapted to this special case, in [9]. As a corollary to Theorem (9.2*), we obtain the following improvement:

COROLLARY. *Let d be an integer such that there is no element of $\pi_{2d+1}(S_{d+1})$ with odd Hopf's invariant. Let M_d be a closed orientable hypersurface in E_{d+1} with self-intersections allowed, and let c be the degree of the Gauss mapping $M_d \to S_d$. Then $c = \chi^*(M)$ modulo 2.*

Let us remark that the condition on d in the Theorem (9.2) (no map with odd Hopf's invariant in $\pi_{2d+1}(S_{d+1})$) is known to be satisfied at least for $d \neq 2^a - 1$, according to J. Adem [1] (explicit proofs in H. Cartan [7]).*

---

* Added in proof: The details of Adem's proof have been recently published in *Algebraic Geometry and Topology*, Princeton University Press, 1957.

According to H. Toda it is satisfied for $d=15$ too (As is well known, H. Hopf has proved that the condition is not satisfied for $d=1,3$ and 7).

Along the same lines, we obtain an extension of a part of N. Steenrod-J. H. C. Whitehead's theorem [13] according to which the d-sphere S_d cannot be parallelizable if $d \neq 2^a - 1$.

THEOREM (9.3). *Any manifold M_d with odd semi-characteristic $\chi^*(M)$ is not parallelizable if $d \neq 2^a - 1$, (in fact, if d is such that every element in $\pi_{2d+1}(S_{d+1})$ has even Hopf's invariant).*

Proof. Suppose M_d is parallelizable. It is known that any regular imbedding of M_d in E_{2d+1} admits in this case a field of normal $(d+1)$-frames F_{d+1}, the corresponding curvatura integra c being zero (see [8], Section 8). Therefore, the semi-characteristic being odd, the corresponding value of γ is $\gamma = c - \chi^*(M) = 1$. Since by Lemma (1.2), γ is the Hopf's invariant mod 2 of some map $S_{2d+1} \rightarrow S_{d+1}$, the dimension d must be of the form $d = 2^a - 1$.

I do not know if there are examples of manifolds M_d with odd semi-characteristic, carrying 2^k fields of mutually orthogonal unit vectors (k being defined by $d+1 = 2^k(2r+1)$).

It was proved in [8] (Corollaire au théorème VIII, § 8), that the real projective space P_d may be immersed into a euclidean space E_{d+n} ($n \geqq d+1$) with a field of normal n-frames if and only if it is parallelizable. The Lemma (1.2) provides a similar (perhaps weaker) statement for a larger class of manifolds:

THEOREM (9.4). *Suppose that the manifold M_d admits a $2m$-fold covering manifold $\bar{M}_d$ with odd semi-characteristic: $\chi^*(\bar{M}_d) = 1 \bmod 2$. Then the manifold M_d cannot be immersed into any euclidean space E_{d+n} with a field of normal n-frames unless there is in $\pi_{2d+1}(S_{d+1})$ some element of odd Hopf's invariant.*

Proof. From an immersion $g: M_d \rightarrow E_{d+n}$ of M_d into some euclidean $(d+n)$-space E_{d+n} with a field F_n of normal n-frames, we obtain by composition with the covering map $p: \bar{M}_d \rightarrow M_d$ a regular immersion $\bar{g}: M_d \rightarrow E_{d+n}$ with a field of normal n-frames $\bar{F}_n$. Let us call $\bar{c}$ the curvatura integra of $\bar{M}_d$ corresponding to $\bar{F}_n$. Because $\bar{g}(\bar{M}_d)$ is homologous to $2m \cdot g(M_d)$ in $V_{d+n,n}$, $\bar{g}$ denoting the composition $\bar{g} = g \circ p$, we have $\bar{c} = 2m \cdot c = 0 \pmod 2$.

Therefore, $\bar{c} - \chi^*(\bar{M}_d) \neq 0$, and because of Theorem (9.2*), $\pi_{2d+1}(S_{d+1})$ must contain some element of odd Hopf's invariant. This completes the proof of Theorem (9.4).

It is known that if S_d is parallelizable, then any manifold M_d which may be immersed in some euclidean space E_{d+n} with a normal n-frame is also parallelizable (see [8], Théorème VIII). In [9], J. Milnor formulates the conjectures that if a parallelizable manifold M_d may be immersed in E_{d+1} in such a way that the Gauss degree be 1, then S_d should be parallelizable.

From Lemma (1.2) follows the

THEOREM (9.5). *If a parallelizable manifold M_d may be immersed in some euclidean space E_{d+n} with a field of normal n-frames inducing an odd curvatura integra, then there is in $\pi_{2d+1}(S_{d+1})$ some element of odd Hopf's invariant.*

Proof. Assuming $n \geqq d+1$, and using the covering homotopy theorem, we may construct on M_d a field G_n of normal n-frames in E_{d+n}, such that the induced curvatura integra is zero (see [8], § 8). Thus the given field and G_n induce different curvatura integra. By Theorem (9.2*), this implies the existence in $\pi_{2d+1}(S_{d+1})$ of an element of odd Hopf's invariant (the question whether this is possible without S_d being parallelizable is unsolved as is well known).

10. Remark. It should be noticed that if one is not interested in the value of the curvatura integra c but only in the fact that c does not depend on the imbedding nor on the normal field (as in Theorem 9.5), then a simpler proof may be given in the case d odd. Let us sketch a "direct" proof of the following weaker form of Theorem (9.2) in this case:

THEOREM (10.1). *If the odd integer d is such that each element of $\pi_{2d+1}(S_{d+1})$ has even Hopf's invariant, then the curvatura integra of any closed differentiable manifold M_d regularly immersed into E_{d+n} with a field of normal n-frames depends only on M_d.*

Proof. Let $M_d{}^i = T^i(M_d)$, $i = 1, 2$ be two regular immersions of the given manifold M_d of dimension d into euclidean spaces E_{d+n_i}. Let $F^i{}_{n_i}$ be two fields $(i = 1, 2)$ of normal n_i-frames on $M_d{}^i$ respectively, inducing maps $\phi^i \colon M_d \to V_{d+n_i, n_i}$ the classes of which are represented by c^i. In order to prove $c^1 = c^2$, let $M_d{}^0 = T^0(M_d)$ be an arbitrary regular *imbedding* of M_d into E_{2d+1} (euclidean $(2d+1)$-space). Consider $E_{d+n_1}, E_{2d+1}, E_{d+n_2}$ as linear subspaces of the euclidean space $E_N = E_{d+n_1} \times E_{2d+1} \times E_{d+n_2}$. Consider on $M_d{}^i$ the fields $F^i{}_{N-d}$ of $(N-d)$-frames normal to $M_d{}^i$, consisting of the vectors of $F^i{}_{n_i}$ followed by $N - d - n_i$ constant unit vectors (mutually orthogonal) normal to E_{d+n_i} in E_N. Each immersion $T^i(M_d)$, $i=1,2$, is isotopic in E_N with $T^0(M_d)$. By the covering homotopy theorem, we obtain on $M_d{}^0$ two fields of normal $(N-d)$-frames in E_N, which we denote again by $\mathbf{F}^i{}_{N-d}$. The curvatura integra corresponding to the mapping $M_d \rightarrow V_{N,N-d}$ induced by the new field $\mathbf{F}^i{}_{N-d}$ on $M_d{}^0$ is c^i.

It is easily seen that $\mathbf{F}^i{}_{N-d}$ may be continuously deformed (keeping the $(N-d)$-frames of $\mathbf{F}^i{}_{N-d}$ normal to $M_d{}^0$ during the deformation), in such a way that the first $(d+1)$ vectors become vectors in E_{2d+1} and the last $N-(2d+1)$ be constant and normal to E_{2d+1}. In other words, we have obtained two fields $\mathbf{F}^i{}_{d+1}$, $i=1,2$, of $(d+1)$-frames normal to $M_d{}^0$ in E_{2d+1}. Moreover, the curvatura integra corresponding to the map $M_d \rightarrow V_{2d+1,d+1}$ induced by $\mathbf{F}^i{}_{d+1}$ (as field over $M_d{}^0$ in E_{2d+1}) is equal to the given c^i which we started from.

Recall that $T^0(M_d)=M_d{}^0$ has been assumed to be an *imbeddding* into E_{2d+1}. According to Section 1 (b), it thus corresponds to $\mathbf{F}^1{}_{d+1}$ and $\mathbf{F}^2{}_{d+1}$ sphere maps f^1, f^2 of S_{2d+1} into S_{d+1}. By assumption, these maps have the same Hopf's invariant mod 2: $h(f^1)=h(f^2) \bmod 2$. It is not difficult to see, that we may change one of the fields, $\mathbf{F}^1{}_{d+1}$ say, without changing c^1 (which is only defined mod 2 because d has been assumed to be odd) in such a way that $h(f^1)=h(f^2)$ as integers. Assume that such a change has been achieved. The Hopf's invariant of f^i is the looping coefficient in E_{2d+1} of $M_d{}^0$ with the locus, $V_d{}^i$ say, of the endpoint of the first vector of the field $\mathbf{F}^i{}_{d+1}$. These looping coefficients being equal, it is possible using again the covering homotopy theorem, to deform $\mathbf{F}^1{}_{d+1}$ and $\mathbf{F}^2{}_{d+1}$ continuously (keeping their unit vectors mutually orthogonal and normal to $M_d{}^0$) in such a way that after the deformation their first vectors coincide. Such a deformation does not change c^1 or c^2.

Let us denote by $\{\mathbf{v}, \mathbf{v}_1{}^i, \mathbf{v}_2{}^i, \cdots, \mathbf{v}_d{}^i\}$ the vectors of $\mathbf{F}^i{}_{d+1}$ (after deformation) and by $\theta^i\colon M_d \rightarrow V_{2d+1,d+1}$ the induced mappings, the classes of which are represented by c^i $(i=1,2)$.

In order to prove $c^1=c^2$, let us first assume that M_d is a parallelizable manifold and let $\mathbf{t}_1, \mathbf{t}_2, \cdots, \mathbf{t}_d$ be a d-field of (mutually orthogonal unit) tangent vectors on $M_d{}^0$. Then each θ^i is homotopic to the map $\theta\colon M_d \rightarrow V_{2d+1,d+1}$ defined by $\theta(x)=\{\mathbf{v}(x), \mathbf{t}_1(x), \mathbf{t}_2(x), \cdots, \mathbf{t}_d(x)\}$. The desired homotopy is given by

$$\theta^i{}_s(x)=\{\mathbf{v}(x), \mathbf{v}_1{}^i(x)\cos(\tfrac{1}{2}\pi s)+\mathbf{t}_1(x)\sin(\tfrac{1}{2}\pi s), \cdots,$$
$$\mathbf{v}_d{}^i(x)\cos(\tfrac{1}{2}\pi s)+\mathbf{t}_d\sin(\tfrac{1}{2}\pi s)\},$$

where $0 \leqq s \leqq 1$. Therefore, if M_d is parallelizable, θ^1 and θ^2 are homotopic and $c^1 = c^2$.

In general, M_d will not be parallelizable. However, if c^1 and c^2 were different, then one of them would be zero (it follows from d being odd, that c^1 and c^2 are remainders mod 2). If $c^i = 0$, $i = 1$ or 2, the corresponding map θ^i is homotopic to zero. By a reasoning of [7] (§ 8), it follows that M_d would be parallelizable.

This completes the "direct" proof of Theorem (10.1).

Appendix.

11. Relative Chern and Pontryagin characteristic classes.

11. a. *Relative Chern classes.*

In this section the coefficients are the *integers*.

Let $\mathfrak{B} = (E_{U(n)}, p, B_{U(n)}, \boldsymbol{U}(n))$ be the classifying bundle for the unitary group of n variables $\boldsymbol{U}(n)$. Suppose that a cross-section θ^r over a closed subset A of $B_{U(n)}$ is given in the associated bundle $\mathfrak{B}^r$ with fibre $W_{n,n-r}$ (the complex Stiefel manifold of $n-r$ complex vectors in C_n).

For $q \geqq r$, the relative Chern class $C_R^{q+1} \in H^{2(q+1)}(B_{U(n)}, A; \boldsymbol{Z})$ corresponding to the cross-section θ^r will be defined by the properties

(11.1) $a^* C_R^{q+1} = C^{q+1}$, the ordinary (absolute) Chern class, a^* being the homomorphism $H^*(B_{U(n)}, A, \boldsymbol{Z}) \rightarrow H^*(B_{U(n)}, \boldsymbol{Z})$ induced by the inclusion $a\colon (B_{U(n)}, 0) \rightarrow (B_{U(n)}, A)$,

(11.2) $\rho^*_{q,n} C_R^{q+1} = 0$, where $\rho^*_{q,n}\colon H^*(B_{U(n)}, A) \rightarrow H^*(B_{U(q)}, \theta^q A)$ is induced by the Borel map $\rho(\boldsymbol{U}(q), \boldsymbol{U}(n))$.

We consider the diagram

$$\begin{tikzcd}
\cdots \arrow[r] & H^q(B_{U(q)}) \arrow[r] & H^q(\theta^q A) \arrow[r, "\delta"] \arrow[d, "\theta^*"] & H^{q+1}(B_{U(q)}, \theta^q A) \arrow[r, "\bar{a}^*"] & H^{q+1}(B_{U(q)}) \arrow[r] & \cdots \\
\cdots \arrow[r] & H^q(B_{U(n)}) \arrow[r] \arrow[u, "\alpha^*"] & H^q(A) \arrow[r, "\delta"] & H^{q+1}(B_{U(n)}, A) \arrow[r, "a^*"] \arrow[u, "\rho^*_{q,n}"] & H^{q+1}(B_{U(n)}) \arrow[r] \arrow[u, "\alpha^*"] & \cdots
\end{tikzcd}$$

where $B_{U(q)}$ is the space of the bundle $\mathfrak{B}^q$ ($B_{U(q)}$ is a classifying space for $\boldsymbol{U}(q)$, thus the notation) and θ^q is the cross-section over A in $\mathfrak{B}^q$ induced by θ^r $(q \geqq r)$.

By considerations similar to those made for the orthogonal group, it is easily seen that α^* is an epimorphism in every dimension and a monomorphism in dimensions not exceeding q. It follows, using exactness and commutativity in the diagram, that if $\rho^*_{q,n}z = 0$ and $a^*z = 0$ for some $z \in H^*(B_{U(n)}, A)$ then z must be zero.

The existence of at least one cohomology class with properties (11.1) and (11.2) is seen as follows: The restriction of C^{q+1} to A is zero because of the assumed existence of a cross-section over A in $\mathfrak{B}^r$. Let $C^{q+1} = a^*x$. Because $0 = \alpha^*C^{q+1} = \alpha^*a^*x = \bar{a}^*\rho^*_{q,n}x$, we have $\rho^*_{q,n}x = \delta\theta^{*-1}y$ for some $y \in H^q(A)$. The class $x - \delta y$ has the properties (11.1) and 11.2).

This proves that properties (11.1) and (11.2) indeed define the relative Chern classes uniquely for the classifying $\boldsymbol{U}(n)$-bundle.

We consider now the more general situation of a $\boldsymbol{U}(n)$-bundle over some compact finite dimensional space X induced by some map $g\colon X \to B_{U(n)}$. Let $(E^r, \pi, X, W_{n,n-r})$ be the associated bundle with fibre $W_{n,n-r}$ and assume a cross-section $\theta^r\colon A \to E^r$ to be given over the closed subset A of X. We may assume $\dim B_{U(n)}$ arbitrarily high. Take $\dim B_{U(n)} \geqq 2 \dim X + 1$ and let $f\colon X \to B_{U(n)}$ be an *injective* map homotopic to g. The bundle induced by f is equivalent to the one induced by g; let us denote it again by $(E^r, \pi, X, W_{n,n-r})$.

Let S be a closed subset of $B_{U(n)}$ containing $f(A)$ and such that there exists a cross-section $\psi\colon S \to B_{U(r)}$ in $\mathfrak{B}^r$, with the property $\psi(a) = \bar{f}\theta(a)$ for every $a \in A$ ($\bar{f}\colon E^r \to B_{U(r)}$ is the bundle map covering $f\colon X \to B_{U(n)}$). Let $c_R{}^{q+1}$ be the $(q+1)$-dimensional relative Chern class of the classifying bundle $\operatorname{mod} S$ obtained using the cross-section $\psi (q \geqq r)$. We shall prove the

LEMMA (11.3). *$f^*c_R{}^{q+1}$ depends only on the homotopy class of the map g inducing the given bundle and on the cross-section θ^r over A.*

Definition. $f^*c_R{}^{q+1} = C_R{}^{q+1} \in H^{2(q+1)}(X, A; \boldsymbol{Z})$ is the relative Chern class (of dimension $2(q+1)$, defined for $q \geqq r$) $\operatorname{mod} A$ of the bundle (E, π, X), corresponding to the cross-section θ^r.

In order to prove Lemma (11.3), we first notice that $f^*c_R{}^{q+1}$ does not depend on S. Indeed, let $i^*\colon H^*(B_{U(n)}, S) \to H^*(B_{U(n)}, f(A))$ be the homomorphism dual to the inclusion $i\colon (B_{U(n)}, f(A)) \to (B_{U(n)}, S)$. We prove that $i^*c_R{}^{q+1}$ is the relative Chern class $\operatorname{mod} f(A)$ corresponding to the restriction ψ_A of ψ over $f(A)$. Consider the diagram

$$\begin{tikzcd}
 & H^{2(q+1)}(B_{U(n)}, fA) & H^{2(q+1)}(B_{U(r)}, \psi S) \arrow[l, "i^*"'] \\
H^{2(q+1)}(B_{U(n)}) & H^{2(q+1)}(B_{U(r)}, \psi f A) \arrow[l, "a^*"'] \arrow[u, "\rho^*_{r,n}"'] & H^{2(q+1)}(B_{U(n)}, S). \arrow[l, "\bar{i}^*"'] \arrow[u, "\rho'^*_{r,n}"']
\end{tikzcd}$$

By commutativity, the relations $\rho^*{}_{r,n}(i^*c_R{}^{q+1}) = 0$ and $a^*(i^*c_R{}^{q+1}) = C^{q+1}$ (showing, by properties (11.1) and (11.2), that $i^*c_R{}^{q+1}$ is indeed the relative Chern class mod fA corresponding to ψ_A) follow from the corresponding relations $\rho'^*{}_{r,n}c_R{}^{q+1} = 0$ and $a'^*c_R{}^{q+1} = c^{q+1}$ for $c_R{}^{q+1}$ (where $a'^* = a^*i^*$). Since $i^*c_R{}^{q+1}$ is independent of S, so is $f^*c_R{}^{q+1}$, since $f^* = f'^*i^*$, where f'^* is induced by $f'\colon (X, A) \to (B_{U(n)}, f(A))$.

It remains to be proved that $f^*c_R{}^{q+1}$ does not depend on the choice of the injective map. Let f_1, f_2 be two injective maps $X \to B_{U(n)}$ homotopic to g. We may assume that $f_1A \cap f_2A = 0$. Otherwise take an injective map $f_0\colon X \to B_{U(n)}$ such that $f_0X \cap f_1X = 0$ and $f_0X \cap f_2X = 0$ (such a map may be obtained taking $\dim B_{U(n)} \geqq 2\dim X + 3$ if necessary) and apply the following proof to f_0 and f_1 first and again to f_0 and f_2. Let S be the union $f_1A \cup f_2A$. The cross-section ψ over S is given by $\psi(a_i) = \theta f_i^{-1}(a_i)$ for $a_i \in f_i(A)$. Denoting by c_{1R} and c_{2R} the relative (universal) Chern classes mod f_1A and f_2A respectively corresponding to the restriction of ψ over f_1A and f_2A, we have to prove $f_1{}^*c_{1R} = f_2{}^*c_{2R}$. By the above remark, we have $f_1{}^*c_{1R} = f_1{}^*c_R$, $f_2{}^*c_{2R} = f_2{}^*c_R$, where c_R is the $2(q+1)$-dimensional class mod S corresponding to ψ. The equality $f_1{}^*c_R = f_2{}^*c_R$ due to $f_1 \simeq f_2$ completes the proof of the Lemma (11.3).

Remark. Similarly to the definition of the Stiefel-Whitney classes, the definition of the relative Chern classes could have been introduced in terms of obstructions to the extension of cross-sections originally given over a subcomplex of the base. The two definitions coincide on their common domain: $\boldsymbol{U}(n)$-bundles $\mathfrak{B}$ over a complex K modulo some subcomplex L. (Use S. Eilenberg's approximation theorem, l.c. section 5).

Naturality property.

LEMMA (11.4). *Let (E, π, X) be a $\boldsymbol{U}(n)$-bundle and let (E', π', X') be the $\boldsymbol{U}(n)$-bundle over X' induced by some map $g\colon X' \to X$. We denote by C'_R and C_R the $2(q+1)$-dimensional relative Chern classes of the bundles (E', π', X') and (E, π, X) respectively, modulo closed subsets $A' \subset X'$ and $A \subset X$ such that $g(A') \subset A$ and corresponding to cross-sections θ and θ' in the associated bundles with fibre $W_{n,n-r}$ $(r \leqq q)$, such that $g\theta'(a') = \theta g(a')$ for every $a' \in A'$. Then $C'_R = g^*(C_R)$.*

Proof. Let $f\colon X \to B_{U(n)}$ be an injective map inducing (E, π, X) and $f'\colon X' \to B_{U(n)}$ be an injective map inducing (E', π', X'). We may assume that $fg(A')$ and $f'(A')$ have no commoon point. Let S be the union $fg(A') \cup f'(A')$ and ψ the cross-section over S in the associated bundle with fibre $W_{n,n-r}$ defined by $\psi f'(a') = \bar{f}'\theta'(a')$ and $\psi fg(a') = \bar{f}\theta g(a')$. Denoting again by c_R the $2(q+1)$-dimensional (universal) relative Chern class modulo S corresponding to ψ, we have $C'_R = f'^*(c_R) = g^*f^*(c_R) = g^*(C_R)$.

Whitney duality. Let $\mathfrak{B}_1$ and $\mathfrak{B}_2$ be two principal bundles with bundle groups $\boldsymbol{U}(n_1)$ and $\boldsymbol{U}(n_2)$ respectively, over the same base space X and let $\theta_1^{r_1}$ and $\theta_2^{r_2}$ be cross-sections over closed subsets A_1 and A_2 (of X) in the associated bundles $\mathfrak{B}_1^{r_1}$ and $\mathfrak{B}_2^{r_2}$ with fibres W_{n_1,n_1-r_1} and W_{n_2,n_2-r_2} respectively. $\theta_1^{r_1}$ and $\theta_2^{r_2}$ determine a cross-section θ^r $(r = r_1 + r_2)$ over $A = A_1 \cap A_2$ in the bundle $\mathfrak{B}^r$, with fibre $W_{n,n-r}$ $(n = n_1 + n_2)$ associated to the Whitney sum $\mathfrak{B} = \mathfrak{B}_1 \oplus \mathfrak{B}_2$.

Denote by C_{iR}^{q+1} the relative Chern class of $\mathfrak{B}_i$, $i = 1, 2$, defined for $q \geqq r_i$, and let C_R^{q+1} be the relative Chern class of $\mathfrak{B}$ defined for $q \geqq r$.

For the relative Chern classes, the Whitney duality takes the form

$$C_R^{q+1} = C_{1_R}^{q+1} + C_{1_R}^{q} \cdot C_2^{1} + \cdots + C_{2_R}^{q+1}. \tag{11.5}$$

In (11.5) some absolute Chern classes occur, however, again, since each product contains at least one relative class, it is itself a relative class.

The proof of formula (11.5) will be based on a theorem similar to Theorem (5.1) stated below (Theorem (11.6)).

Relative Chern classes as symmetric functions. Let $(E, p, X, \boldsymbol{U}(n))$ be a principal $\boldsymbol{U}(n)$-bundles over a compact finite dimensional space X. Consider the subgroup $\boldsymbol{Q}(n) = \boldsymbol{U}(1) \times \boldsymbol{U}(1) \times \cdots \times \boldsymbol{U}(1)$, n factors, of $\boldsymbol{U}(n)$ and the "space of flags" $\bar{X} = E/\boldsymbol{Q}(n)$ over X. We have a fibering $\rho\colon \bar{X} \to X$ induced by the projection $p\colon E \to X$ and the cross-section θ^r over $A \subset X$ may be used to construct a subset $\bar{A} \subset \bar{X}$ as follows. Let $E^r = E/\boldsymbol{U}(r)$ be the space of the bundle with fibre $W_{n,n-r}$ associated to $(E, p, X, \boldsymbol{U}(n))$. We have the diagram

$$\begin{tikzcd}
\bar{A} \arrow[r, "\bar{\theta}"] \arrow[d, "\rho_A"] & \bar{E}^r \arrow[r, "\omega"] \arrow[d, "\rho_E"] & \bar{X} \arrow[d, "\rho_X"] \\
A \arrow[r, "\theta"'] & E^r \arrow[r, "p"'] & X
\end{tikzcd}$$

where $\bar{E}^r$ is the space of flags over E^r (i.e. $E/\boldsymbol{Q}(r) = \bar{E}^r$) and $\rho_E\colon \bar{E}^r \to E^r$ is induced by $\boldsymbol{Q}(r) \subset \boldsymbol{U}(r)$. The bundle $(\bar{A}, \rho_A, A, \boldsymbol{F}(r), \boldsymbol{U}(r))$ is induced by $\theta\colon A \to E^r$. The principal bundle $\mathfrak{E} = (E, \pi, \bar{X}, \boldsymbol{Q}(n))$ is the Whitney sum $\mathfrak{E} = \mathfrak{E}^1 \oplus \mathfrak{E}^2 \oplus \cdots \oplus \mathfrak{E}^n$ of n principal bundles $\mathfrak{E}^i$ with group $\boldsymbol{U}(1)$. Let $x_i \in H^2(\bar{X}; \boldsymbol{Z})$ be the 2-dimensional (only non-zero positive dimensional)

Chern class of $\mathfrak{E}^i$. For $r+1 \leqq i \leqq n$, the relative Chern class mod $\bar{A}$ of $\mathfrak{E}^i$ may be defined (using the cross-section over $\bar{A}$ in $\mathfrak{E}^i$ induced by θ^r). Let $x_{r+1}, x_{r+2}, \cdots, x_n$ mean the *relative* classes. Then the elementary symmetric function $S^{q+1}(x_1, \cdots, x_n)$ is a relative class for $q \geqq r$ (each product of $q+1$ distinct factors from the $x_1, \cdots, x_n$ must contain at least one of the variables $x_{r+1}, \cdots, x_n$). Let us denote by $S_R^{q+1}(x_1, \cdots, x_n)$ this relative class. We have the theorem

THEOREM (11.6). *Let* $\rho_R^*\colon H^*(X, A; \mathbf{Z}) \to H^*(\bar{X}, \bar{A}; \mathbf{Z})$ *be the homomorphism induced by* $\rho_R\colon (\bar{X}, \bar{A}) \to (X, A)$. *Then,*

(a) ρ_R^* *is a monomorphism,*

(b) $\rho_R^* C_R^{q+1} = S_R^{q+1}(x_1, \cdots, x_n)$ *for* $q \geqq r$.

The proof is very similar to the proof of Theorem (5.1). We are not going to enter into the details again. Along the same lines as for the proof of (5.1), we need the result

$$H^*(\boldsymbol{F}(n); \mathbf{Z}) = \mathbf{Z}[x_1, \cdots, x_n]/(S^+(x_1, \cdots, x_n)),$$

with $\boldsymbol{F}(n) = \boldsymbol{U}(n)/\boldsymbol{Q}(n)$, where $(S^+(x_1, \cdots, x_n))$ denotes the ideal generated in $\mathbf{Z}[x_1, \cdots, x_n]$ by the symmetric functions of positive degree (see [3], Proposition 31.1). The only points where the method of proof of (5.1) breaks down now are those where use was made of the fact that the coefficient ring for Stiefel-Whitney classes was a *field* ($\mathbf{Z}_2$).

The assertion that the term E_2 in the spectral sequence of $\rho\colon \bar{X} \to X$ reduces to $H^*(X) \otimes H^*(\boldsymbol{F}(n))$ is, however, still true because $\boldsymbol{F}(n) = \boldsymbol{U}(n)/\boldsymbol{Q}(n)$ has no torsion.

The only non-trivial change is that it is no longer obvious that $H^*(X; \mathbf{Z})$ should be (at least additively) isomorphic to E_∞. This proves, however, tc hold, as will be seen from the following argument I learned from A. Borel, similar to an argument by J. P. Serre ([10], Chap. III, 7, Prop. 9).

LEMMA (11.7). *Let* $\sigma\colon H^*(F) \to H^*(E)$ *be a right-inverse (additive) homomorphism to* $i^*\colon H^*(E) \to H^*(F)$, *where* E *is the space of a bundle* (E, π, B, F) *with fibre* F *and* i *the inclusion* $i\colon F \to E$. *Assume that either* B *or* F *has no torsion. Then* $H^*(E)$ *is isomorphic to* $H^*(B) \otimes H^*(F)$. *Moreover, the isomorphism preserves the product if* σ *does.* (In this lemma the domain of coefficients is any commutative ring with unit).

Proof. Let $\omega\colon H^*(B) \otimes H^*(F) \to H^*(E)$ be the linear map defined by $\omega(x \otimes f) = \pi^*(x) \cdot \sigma(f)$. We are going to prove that ω is an isomorphism which preserves products if σ does.

We first notice that ω preserves the filtration: $H^*(B) \otimes H^*(F)$ being filtered by the ideals $A^q = \sum_{i \geqq q} H^i(B) \otimes H^*(F)$ and $H^*(E)$ by the ideals $J^q = \pi^*(\sum_{i \geqq q} H^i(B)) \cdot H^*(E)$. We have for every $q, \omega(A^q) \subset J^q$. Therefore, ω induces an additive homomorphism $\bar{\omega}$ of the corresponding graded rings $\sum A^q/A^{q+1}$ into $\sum J^q/J^{q+1}$, where $\sum$ denotes the direct sum. It is well known and easily seen that ω is an isomorphism if $\bar{\omega}$ is.

By triviality of the spectral sequence of the fibering $p: E \rightarrow B$ (because $i^*: H^*(E) \rightarrow H^*(F)$ which admits a right inverse, is an epimorphism), it follows that $E_2 = H^*(B, H^*(F))$ is isomorphic to the graded ring E_∞ associated to $H^*(E)$, i. e. $\sum J^q/J^{q+1}$. Let k be this isomorphism ($k^2{}_\infty$ with the notations of [3], § 1).

Since either B or F has no torsion by assumption, $E_2 = H^*(B) \otimes H^*(F)$; identifying $\sum A^q/A^{q+1}$ with $H^*(B) \otimes H^*(F)$ in the natural manner, the lemma will be proved by showing that $\bar{\omega}: H^*(B) \otimes H^*(F) \rightarrow E_\infty$ is identical to the map $k: H^*(B) \otimes H^*(F) \rightarrow E_\infty$.

Let $x \otimes f \in H^*(B) \otimes H^*(F)$, where $x \in H^p(B)$, $f \in H^q(F)$. We have $\omega(x \otimes f) = \pi^*(x) \cdot \sigma(f) \in J^{p,q} = \pi^*(\sum_{i \geqq p} H^i(B)) \cdot H^q(E)$, and $\bar{\omega}(x \otimes f)$ is the image of $\omega(x \otimes f)$ in $J^{p,q}/J^{p+1,q-1} = E_\infty{}^{p,q}$. By definition of the product in E_∞, we obviously have $\bar{\omega}(x \otimes f) = \bar{\omega}(x \otimes 1) \cdot \bar{\omega}(1 \otimes f)$. Since k has also this property, it is sufficient to verify $\bar{\omega} = k$ on the elements of the form $x \otimes 1$ and $1 \otimes f$.

$\bar{\omega}(x \otimes 1) = \pi^*(x) \in J^{p,0}$ $(J^{p+1,-1} = 0)$. We have $k(x \otimes 1) = \pi^*(x)$. See [3], § 4, (b).

$\bar{\omega}(1 \otimes f) = \overline{\sigma(f)}$, where $\overline{\sigma(f)}$ represents the image of $\sigma(f) \in J^{0,q}$ in $J^{0,q}/J^{1,q-1}$. By [3], § 4 (c), we have $k^{-1}(\overline{\sigma(f)}) = 1 \otimes i^*\sigma(f) = 1 \otimes f$ since σ is a right inverse to i^*. Thus, again $\bar{\omega}(1 \otimes f) = k(1 \otimes f)$.

If σ preserves the product, then

$$\begin{aligned} \omega[(x \otimes f) \cdot (x' \otimes f')] &= (-1)^{qp'} \omega(xx' \otimes ff') = (-1)^{qp'} \pi^*(x \cdot x') \cdot \sigma(f \cdot f') \\ &= (-1)^{qp'} \pi^*(x) \cdot \pi^*(x') \cdot \sigma(f) \cdot \sigma(f') = \pi^*(x) \cdot \sigma(f) \cdot \pi^*(x') \cdot \sigma(f') \\ &= \omega(x \otimes f) \cdot \omega(x' \otimes f'). \end{aligned}$$

In the situation of Theorem (11.6), the existence of the homomorphism σ is obvious (one has $H^*(\boldsymbol{F}(n); \mathbf{Z}) = \mathbf{Z}[u_1, \cdots, u_n]/(S^+(u_1, \cdots, n_n))$, where $u_k = i^* x_k$; let $h_1 = 1, h_2, \cdots, h_t$ be a basis for the vector space

$H^*(\boldsymbol{F}(n);\boldsymbol{Z})$, the h_i being represented by polynomials $P_i(u_1,\cdots,u_n)$ in $u_1,\cdots,u_n$, and define $\sigma(h_i)$ as the polynomial in $x_1,\cdots,x_n$ obtained from P_i by the substitution $u_k \to x_k$; extend then σ by linearity). This completes the proof of Theorem (11.6) part (a).

The proof of part (b) is similar to the proof of (b) in Theorem (5.1). Use has to be made of the results of [6] (in particular Prop. 4.1) rather than from [4]. A slight change occurs at the end of the proof: we have to show that $\mu_R^* S_R^{q+1}(x_1,\cdots,x_n) = 0$, where $\mu_R^*\colon H^*(B_{Q(n)},\bar{A}) \to H^*(B_{Q(r)},\bar{A}^1)$. The argument used for Stiefel-Whitney classes does not work now, because $\deg x_i = 2$ and $a^*\colon H^2(B_{Q(r)},\bar{A}^1) \to H^2(B_{Q(r)})$ need not be a monomorphism. However, $\mu_R^* x_{r+j} = 0$ for $j = 1,\cdots,n-r$ may be seen as follows. Consider for some j $(1 \leqq j \leqq n-r)$ the $\boldsymbol{U}(1)$-bundle $\mathfrak{E}^{r+j}$ over $B_{Q(n)}$; it admits over $\bar{A}$ the section θ_j. The map $\mu\colon B_{Q(r)} \to B_{Q(n)}$ induces over $B_{Q(r)}$ a $\boldsymbol{U}(1)$-bundle ("counter-image of $\mathfrak{E}^{r+j}$") and explicit construction shows that the induced cross-section ψ over $\bar{A}^1$ (defined by $\psi(u) = (u, \theta_j\mu(u))$) can be extended all over $B_{Q(r)}$. Thus, by naturality, $\mu_R^* x_{r+j} = 0$ (from this $\mu_R^* S_R^{q+1}(x_1,\cdots,x_n) = 0$ follows because of $q \geqq r$).

11. b. *Relative Pontryagin classes.*

From now on, the coefficients are integers mod p, where p is prime and > 2. The following definition and naturality property would be valid without alteration with integer coefficients, but Whitney duality is not.

Let $\mathfrak{B} = (E, p, X, \boldsymbol{SO}(n))$ be a principal $\boldsymbol{SO}(n)$-bundle induced by a map $\tau\colon X \to B_{\boldsymbol{SO}(n)}$. Let $\sigma\colon B_{\boldsymbol{SO}(n)} \to B_{\boldsymbol{U}(n)}$ be the mapping corresponding to the inclusion $\boldsymbol{SO}(n) \to \boldsymbol{U}(n)$. Then $\sigma \circ \tau$ induces over X a principal $\boldsymbol{U}(n)$-bundle $\mathfrak{B}_C = (E_C, \pi, X, \boldsymbol{U}(n))$.

Let θ^r be a cross-section over the closed subset A of X in the bundle $\mathfrak{B}^r$ associated to $\mathfrak{B}$ with fibre $V_{n,n-2r+1}$. For $k \geqq r$, we have a cross-section θ^k over A in $\mathfrak{B}^k$ (with fibre $V_{n,n-2k+1}$) induced by θ^r. These cross-sections provide cross-sections $\bar{\theta}_C{}^k$ over A in the corresponding "complex" bundles $\mathfrak{B}_C{}^k$,associated to $\mathfrak{B}_C$ with fibre $W_{n,n-2k+1}$) as follows. Let $\bar{\tau}$, $\bar{\sigma}$ be the maps of the total space covering τ, σ respectively ($\bar{\sigma}$ is not a bundle map), and let h be the bundle map covering $\sigma \circ \tau$. Then h is injective (actually a homeomorphism) on each fibre $W_{n,n-2k+1}$, and $\theta_C{}^k$ may be defined by

$$(11.8) \qquad \pi\theta_C{}^k(a) = a, \qquad \theta_C{}^k(a) = h^{-1}\overline{\sigma\tau}\theta^k(a)$$

Definition. The $4k$-dimensional relative Pontryagin class

$$P_R{}^k \in H^{4k}(X, X; \boldsymbol{Z}_p) \bmod A$$

corresponding to the cross-section θ^r, defined for $k \geqq r$, is given by

$$P_R^k = (-1)^k C_R^{2k}, \tag{11.9}$$

where C_R^{2k} is the relative Chern class mod A of $\mathfrak{B}_C$ corresponding to θ_C^k.

Naturality. Let $\mathfrak{B}$, $\mathfrak{B}'$ be two $\boldsymbol{SO}(n)$-bundles over X and X' respectively, such that $\mathfrak{B}$ is induced from $\mathfrak{B}'$ by a map $f\colon X \to X'$. Let $\mathfrak{B}^k = (E^k, X)$, $\mathfrak{B}'^k = (E'^k, X')$ be the associated bundles with fibre $V_{n,n-2k+1}$ and assume that cross-sections θ^r, θ'^r in $\mathfrak{B}^r$, $\mathfrak{B}'^r$ are given over closed subsets $A \subset X$, $A' \subset X'$ respectively, such that $f(A) \subset A'$ and $\theta' f(a) = \bar{f}\theta(a)$, ($\bar{f}\colon E^k \to E'^k$ cover f) for every $a \in A$.

Let P^k and P'^k be the relative Pontryagin classes ($k \geqq r$) of $\mathfrak{B}$ and $\mathfrak{B}'$ corresponding to θ and θ' respectively. Then

$$P^k = f^*(P'^k). \tag{11.10}$$

Proof. The above formula follows from the naturality property of relative Chern classes, provided we prove that $f_C\theta_C(a) = \theta'_C f(a)$, where $f_C\colon E_C^k \to E_C'^k$ covers f (Remark that (E_C^k, X) is induced from (E'^k_C, X') by $f\colon X \to X'$). We have

$$h\theta'_C f(a) = \bar{\sigma}\tau\theta' f(a) = \bar{\sigma}\tau\bar{f}\theta(a) = hf_C\theta_C(a)$$

and, since h is homeomorphic on the fibres,

$$\theta'_C f(a) = f\ \theta_C(a) \text{ for every } a \in A.$$

We are thus in position to apply the naturality property of relative Chern classes and (11.10) follows.

Whitney *duality* for Pontryagin classes will follow from Whitney duality for relative Chern classes reduced mod p. Because of the naturality property, we may restrict attention to the case of a classifying $\boldsymbol{SO}(n)$ bundle $\mathfrak{B} = (E_{SO(n)}, p, B_{SO(n)}, \boldsymbol{SO}(n))$ assuming a cross-section to be given over A (closed subset of $B_{SO(n)}$) in the associated bundle $\mathfrak{B}^r$ with fibre $V_{n,n-2r+1}$. Let $\mathfrak{B}_C$ be the $\boldsymbol{U}(n)$-bundle over $B_{SO(n)}$ induced by $\sigma\colon B_{SO(n)} \to B_{U(n)}$, and let θ_C^r be the cross-section over A induced by θ^r in the bundle $\mathfrak{B}_C^r$ associated to $\mathfrak{B}_C$ with fibre $W_{n,n-2r+1}$.

LEMMA (11.11). *The* $(4i+2)$*-dimensional relative Chern classes of* $\mathfrak{B}_C \bmod A$ *corresponding to* θ_C^r *are zero* mod p: $C_R^{2i+1} = 0$, $i \geqq r$.

Proof. Consider the diagram

$$(11.12)\quad \begin{tikzcd} H^{4i+1}(E) \arrow[r, "\bar{\imath}^*"] & H^{4i+1}(\theta^i A) \arrow[r, "\delta"] \arrow[d, "\theta^*"] & H^{4i+2}(E^i, \theta^i A) \arrow[r] & H^{4i+2}(E^i) \\ H^{4i+1}(B_{SO(n)}) \arrow[u, "\omega^*"] \arrow[r, "i^*"] & H^{4i+1}(A) \arrow[r, "\delta"] & H^{4i+2}(B_{SO(n)}, A) \arrow[u, "\omega_R^*"] \arrow[r, "a^*"] & H^{4i+2}(B_{SO(n)}). \arrow[u, "\omega^*"] \end{tikzcd}$$

Since $a^*(C_R^{2i+1}) = C^{2i+1}$, we have (by [5], Proposition 25.4) $a^* C_R^{2i+1} = 0$ (coefficients mod p). Therefore $C_R^{2i+1} = \delta x$, $x \in H^{4i+1}(A; \mathbf{Z}_p)$, and since θ^* is an isomorphism, there exists a class $u \in H^{4i+1}(\theta^i A)$, with $\theta^* u = x$. We have

$$\delta u = \delta \theta^{*-1} x = \omega_R^* \delta x = \omega_R^* C_R^{2i+1} = 0.$$

The last equality follows from consideration of the diagram

$$\begin{tikzcd} H^{4i+2}(E^i, \theta^i A) & H^{4i+2}(E_C^i, \theta_C^i A) \arrow[l, "\bar{\sigma}^*"'] \\ H^{4i+2}(B_{SO(n)}, A) \arrow[u, "\omega_R^*"] & H^{4i+2}(B_{U(n)}, A). \arrow[l, "\sigma^*"'] \arrow[u, "\pi^*"'] \end{tikzcd}$$

Indeed, $\omega_R^* C_R^{2i+1} = \omega_R^* \sigma^* c_R^{2i+1} = \bar{\sigma}^* \pi^* c_R^{2i+1} = 0$ (by (11.4)).

By exactness of the rows in diagram (11.12), there exists an element $z \in H^{4i+1}(E^i)$ such that $\bar{\imath}^* z = u$. The assertion $C_R^{2i+1} = 0$ follows from the fact that ω^* is an *epimorphism* in every dimension (By [5], Theorem 23.2, $H^*(B_{SO(2m-1)}; \mathbf{Z}_p) = \mathbf{Z}_p[P_1, \cdots, P_{m-1}]$ and

$$H^*(B_{SO(2m)}; \mathbf{Z}_p) = \mathbf{Z}_p[P_1, \cdots, P_{m-1}, W_{2m}].$$

Notice that E^i is classifying space for $\mathbf{SO}(2i-1)$.).

Remark. Using the fact that ω^* is still an epimorphism if *integer* coefficients are used (see a forthcoming paper by A. Borel and F. Hirzebruch), the same method would give $2C_R^{2i+1} = 0$, where C_R^{2i+1} is the integer relative Chern class of a $\mathbf{U}(n)$-bundle obtained from an $\mathbf{SO}(n)$-bundle.

Whitney duality for relative Pontryagin classes is an immediate consequence of the same property for relative Chern classes with coefficients mod p, making use of Lemma (11.11).

Let $\mathfrak{B}_i$ be two $\mathbf{SO}(n_i)$-bundles $(i = 1, 2)$ over X and let θ_i be cross-sections over (closed subsets) $A_i \subset X$ in the associated bundles $\mathfrak{B}_i^{r_i} = (E_i^{r_i}, p_i, X, V_{n_i, n_i - 2r_i + 1})$.

Let $\mathfrak{B} = \mathfrak{B}_1 \oplus \mathfrak{B}_2$ be the Whitney sum and θ the cross-section over $A = A_1 \cap A_2$ in $\mathfrak{B}^r$ (with fibre $V_{n,n-2r+1}$, where $n = n_1 + n_2$, $r = r_1 + r_2$) obtained using $\theta_1{}^{r_1}$ and $\theta_2{}^{r_2}$.

$P_R{}^k$, the relative Pontryagin class of dimension $4k$ of corresponding to θ is defined for $k \geqq r$. Similarly, $P^1{}_R{}^k$, $P^2{}_R{}^k$ are defined for $k \geqq r_1$ and $k \geqq r_2$ respectively.

One has in $H^{4k}(X, A; \boldsymbol{Z}_p)$:

$$P_R{}^k = P^1{}_R{}^k + \cdots + P^1{}_R{}^{r_1} \cdot P^2{}_R{}^{k-r_1} + \cdots + P^2{}_R{}^k \qquad (k \geqq r). \tag{11.13}$$

Although some absolute classes might appear in the above formula, each cup-product contains at least one relative class. The sum on the right consists only of *relative* classes.

Pontryagin classes as symmetric functions. Consider again a principal $\boldsymbol{SO}(n)$-bundle $\mathfrak{B} = (E, p, X, \boldsymbol{SO}(n))$ and define the subgroup $\boldsymbol{Q}(n)$ of $\boldsymbol{SO}(n)$ by $\boldsymbol{Q}(n) = \boldsymbol{SO}(2) \times \boldsymbol{SO}(2) \times \cdots \times \boldsymbol{SO}(2)$ or $\boldsymbol{Q}(n) = \boldsymbol{SO}(2) \times \boldsymbol{SO}(2) \times \cdots \times \boldsymbol{SO}(2) \times \boldsymbol{SO}(1)$ according as $n = 2m$ or $n = 2m+1$ (m factors $\boldsymbol{SO}(2)$ in both cases). Consider the quotient space $E/\boldsymbol{Q}(n)$. The principal fibre bundle $(E, \pi, E/\boldsymbol{Q}(n), \boldsymbol{Q}(n))$ is the Whitney sum of m principal $\boldsymbol{SO}(2)$-bundles $\mathfrak{E}^1, \mathfrak{E}^2, \cdots, \mathfrak{E}^m$. Let $x_1, x_2, \cdots, x_m$ be their Chern classes ($\boldsymbol{SO}(2)$ being identified with $\boldsymbol{U}(1)$).

Assuming a cross-section θ over $A \subset X$ (closed subset) to be given in $\mathfrak{B}^r = (E^r, p, X, V_{n,n-2r+1})$ we obtain cross-sections in $\mathfrak{E}^1$ for $i = r, r+1, \cdots, m$ over $\bar{A} \subset B_{\boldsymbol{Q}(n)}$ as follows: E^r is the base space of a principal $\boldsymbol{SO}(2r-1)$-bundle $(E, E^r, \boldsymbol{SO}(2r-1))$. Let $\bar{E}^r$ be the space of flags over $\bar{E}^r$, i.e. $\bar{E}^r = E/\boldsymbol{Q}(2r-1)$, where $\boldsymbol{Q}(2r-1)$ is the subgroup of $\boldsymbol{SO}(n)$ consisting of the matrices of the type

$$\begin{bmatrix} D_1 & & & & & & & \\ & \cdot & & & & 0 & & \\ & & \cdot & & & & & \\ & & & \cdot & & & & \\ & & & & D_{r-1} & & & \\ & 0 & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & \cdot & \\ & & & & & & & \cdot \\ & & & & & & & \cdot \\ & & & & & & & & 1 \end{bmatrix}, \text{ where } D_i = \begin{bmatrix} \cos(2\pi x_i) & \sin(2\pi x_i) \\ -\sin(2\pi x_i) & \cos(2\pi x_i) \end{bmatrix}.$$

We have the diagram

(11.14)
$$\begin{tikzcd}
 & \bar{E}^r \arrow[r, "\omega"] \arrow[d, "\rho_E"'] & \bar{X} \arrow[d, "\rho_X"] \\
A \arrow[r, "\theta"] & E^r \arrow[r, "p"] & X
\end{tikzcd}$$

The map $\omega\colon \bar{E}^r \to \bar{X}$ is induced by the identity $E \to E(\boldsymbol{Q}(2r-1) \subset \boldsymbol{Q}(n))$. Let $\bar{A}$ be the space of the bundle $(\bar{A}, \rho_A, A, \boldsymbol{F}(2r-1), \boldsymbol{SO}(2r-1))$ induced by θ. Notations: $\boldsymbol{F}(2r-1) = \boldsymbol{SO}(2r-1)/\boldsymbol{Q}(2r-1)$, $\bar{\theta}\colon \bar{A} \to \bar{E}^r$ is the bundle map covering θ. The maps $p\theta$ and $\omega\bar{\theta}$ are injective and we may consider $\bar{A}$ as a subset of $\bar{X}$. Geometrically, a point of $\bar{A} \subset \bar{X}$ consists of a point a of A together with a sequence of m oriented 2-planes $\pi_1, \pi_2, \cdots, \pi_m$, such that π_r contains the first, π_{r+1} the second and the third, $\cdots$, π_m the $(n-2r)$-th and the $(n-2r+1)$-st vectors of $\theta(a)$, assuming $n = 2m$. If $n = 2m+1$, π_r contains the first and second, etc., π_m the $(n-2r)$-th and the $(n-2r+1)$-st vectors of $\theta(a)$. In both cases ($n = 2m$ or $2m+1$), since π_r is oriented, $\mathfrak{E}^r$ admits a cross-section over $\bar{A}$ and so do $\mathfrak{E}^{r+1}, \cdots, \mathfrak{E}^m$. We define $x_r, x_{r+1}, \cdots, x_m$ (the characteristic classes of $\mathfrak{E}^r, \cdots, \mathfrak{E}^m$) as *relative* classes corresponding to the cross-sections given by θ over $\bar{A}$. The elementary symmetric functions $S^k(x_1^2, \cdots, x_m^2)$ are then relative classes $\bmod \bar{A}$ (of dimension $4k$) for $k \geqq r$ and will, consequently, be denoted by $S_R^k(x_1^2, \cdots, x_m^2)$. One has the

THEOREM (11.15). *Let* $\rho_R^*\colon H^*(X, A; \boldsymbol{Z}_p) \to H^*(\bar{X}, \bar{A}; \boldsymbol{Z}_p)$ *be the homomorphism induced by* $\rho_R\colon (\bar{X}, \bar{A}) \to (X, A)$. *Then* (a) ρ_R^* *is a monomorphism, and* (b) $\rho_R^* P_R^k = S_R^k(x_1^2, \cdots, x_m^2)$ *for* $k \geqq r$.

Proof of (a). Consider the diagram

$$\begin{tikzcd}
H^{4k-1}(\bar{X}) \arrow[r, "\bar{i}^*"] & H^{4k-1}(\bar{A}) \arrow[r, "\delta"] & H^{4k}(\bar{X}, \bar{A}) \arrow[r, "\bar{a}^*"] & H^{4k}(\bar{X}) \\
H^{4k-1}(X) \arrow[r, "i^*"] \arrow[u, "\rho_X^*"] & H^{4k-1}(A) \arrow[r, "\delta"] \arrow[u, "\rho_A^*"] & H^{4k}(X, A) \arrow[r, "a^*"] \arrow[u, "\rho_R^*"] & H^{4k}(X) \arrow[u, "\rho_X^*"]
\end{tikzcd}$$

(coefficients $=$ remainders $\bmod p$, $p = \text{prime} > 2$), where ρ_X^* and ρ_A^* are monomorphisms in every dimension (see [5], Theorem 23.2) and i, $\bar{i}$ are the inclusions $i = p\theta$, $\bar{i} = \omega\bar{\theta}$.

The situation is entirely similar to the one in the proof of Theorem (5.1). A straightforward exactness argument shows that (a) follows from the Lemma: *If* $b \in H^*(A)$ *and* $w \in H^*(\bar{X})$ *are such that* $\rho_A^* b = \bar{i}^* w$, *then there exists a class* $v \in H^*(X)$, *such that* $i^* v = b$.

The proof of the lemma is entirely similar to the one given in the proof of Theorem (5.1).

Proof of (b). By naturality, it is sufficient to prove the formula $\rho_R{}^*P_R{}^k = S_R{}^k(x_1{}^2,\cdots,x_m{}^2)$ for the bundle $\mathfrak{B} = (B_{Q(n)},\rho_n,B_{SO(n)},\boldsymbol{F}(n),\boldsymbol{SO}(n))$ obtained from the classifying bundle ($B_{Q(n)}$ is the space of flags over $B_{SO(n)}$). The diagram (11.14) reads in this case.

$$\begin{tikzcd}
A \arrow[r, "\bar\theta"] \arrow[d, "\rho_A"] & B_{SO(2r-1)} \arrow[r, "\mu"] \arrow[d, "\rho_{2r-1}"] & B_{Q(n)} \arrow[d, "\rho_n"] \\
\bar A \arrow[r, "\theta"] & B_{Q(2r-1)} \arrow[r, "p"] & B_{SO(n)}
\end{tikzcd}$$

and there is a similar diagram with k substituted for r for every k such that $r \leqq k \leqq \frac{1}{2}(n+1)$. Considering $\bar A$ as a subset of $B_{Q(2r-1)}$ and $B_{Q(n)}$ by the injections $\bar\theta$ and $\mu\bar\theta$, we have the following diagram

$$\begin{tikzcd}
H^{4k-1}(B_{Q(2k-1)}) \arrow[r, "\bar\theta^*"] & H^{4k-1}(\bar A) \arrow[r, "\delta"] & H^{4k}({}_{Q(2k-1)},\bar A) \arrow[r, "a^*"] & H^{4k}(B_{Q(2k-1)}) \\
H^{4k-1}(B_{Q(n)}) \arrow[r, "\theta^*"] \arrow[u, "\mu^*"] & H^{4k-1}(\bar A) \arrow[r, "\delta"] \arrow[u, leftrightarrow, "\cong"] & H^{4k}(B_{Q(n)},\bar A) \arrow[r, "a^*"] \arrow[u, "\mu_R{}^*"] & H^{4k}(B_{Q(n)}). \arrow[u, "\mu^*"]
\end{tikzcd}$$

From the relation $\rho^*(P^k) = S^k(x_1{}^2,\cdots,x_m{}^2)$ for the absolute Pontryagin classes, (see [6], Proposition 5.1), we have $a^*y = 0$, setting $y = \rho_R{}^*P_R{}^k - S_R{}^k(x_1{}^2,\cdots,x_m{}^2)$. Indeed, $a^*P_R{}^k = P^k$ is immediately seen from the definition and the corresponding equality for Chern classes.

By an exactness argument used several times in this paper, (b) follows from $\mu_R{}^*y = 0$. The proof of $\mu_R{}^*S_R{}^k(x_1{}^2,\cdots,x_m{}^2) = 0$ is similar to the one given for Chern classes. The equality $\mu_R{}^*\rho_R{}^*P_R{}^k = 0$ follows from consideration of the diagram

$$\begin{tikzcd}
H^{4k}(B_{Q(2k-1)},\bar A) & H^{4k}(B_{Q(n)},\bar A) \arrow[l, "\mu_R{}^*"'] \\
H^{4k}(B_{SO(2k-1)},A) \arrow[u, "\kappa_R{}^*"] & H^{4k}(B_{SO(n)},A). \arrow[l, "p^*"'] \arrow[u, "\rho_R{}^*"']
\end{tikzcd}$$

One has $\mu_R{}^*\rho_R{}^*P_R{}^k = \kappa_R{}^*p^*P_R{}^k$. Now, $p^*(P_R{}^k) = 0$ because

$$P_R{}^k = (-1)^k\sigma^*(C_R{}^{2k})$$

and of the diagram

$$\begin{tikzcd}
H^{4k}(B_{SO(2k-1)}, A) & H^{4k}(B_{U(2k-1)}, \bar{\sigma}A) \arrow[l, "\bar{\sigma}^*"'] \\
H^{4k}(B_{SO(n)}, A) \arrow[u, "p^*"'] & H^{4k}(B_{U(n)}, A) \arrow[l, "\sigma^*"'] \arrow[u, "\pi^*"']
\end{tikzcd}$$

$p^*(P_R^k) = (-1)^k p^*\sigma^*(C_R^{2k}) = (-1)^k\bar{\sigma}^*\pi^*(C_R^{2k}) = 0$, by definition of the relative Chern classes.

This completes the proof of Theorem (11.15).

MASSACHUSETTS INSTITUTE OF TECHNOLOGY.

REFERENCES.

[1] J. Adem, "The iteration of the Steenrod squares in algebraic topology," *Proceedings of the National Academy of Science*, U. S. A., vol. 38 (1952), pp. 720-726.

[2] P. Alexandroff and H. Hopf, *Topologie*, Springer, 1935.

[3] A. Borel, "Sur la cohomologie des espaces fibrés principaux et des espaces homogènes de groupes de Lie compacts," *Annals of Mathematics*, vol. 57 (1953), pp. 115-207.

[4] ———, "La cohomologie mod 2 de certains espaces homogènes," *Commentarii Mathematici Helvetici*, vol. 27 (1953), pp. 165-197.

[5] ———, "Selected topics in the homology theory of fibre bundles," Mimeographed notes, Chicago, 1954.

[6] A. Borel and J. P. Serre, "Groupes de Lie et puissances réduites de Steenrod," *American Journal of Mathematics*, vol. 75 (1953), pp. 409-448.

[7] H. Cartan, "Sur l'itération des opérations de Steenrod," *Commentarii Mathematici Helvetici*, vol. 29 (1955), pp. 40-58.

[8] M. Kervaire, "Courbure intégrale généralisée et homotopie," *Mathematische Annalen*, vol. 131 (1956), pp. 219-252.

[9] J. Milnor, "On the immersion of n-manifolds in $(n+1)$-space," *Commentarii Mathematici Helvetici*, vol. 30 (1956), pp. 275-284.

[10] J. P. Serre, "Homologie singulière des espaces fibrés," *Annals of Mathematics*, vol. 54 (1951), pp. 425-505.

[11] N. Steenrod, "Cohomology invariants of mappings," *Annals of Mathematics*, vol. 50 (1949), pp. 954-988.

[12] ———, *Topology of fibre bundles*, Princeton Press, 1950.

[13] N. Steenrod and J. H. C. Whitehead, "Vector fields on the n-sphere," *Proceedings of the National Academy of Science*, vol. 37 (1951), pp. 58-63.

[14] R. Thom, "Quelques propriétés globales des variétés différentiables," *Commentarii Mathematici Hedvetici*, vol. 28 (1954), pp. 17-86.

[15] H. Whitney, "Differentiable manifolds," *Annals of Mathematics*, vol. 37 (1936), pp. 645-680.

[16] W. T. Wu, "Classes caractéristiques et i-carrés dans une variété," *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences*, Paris, vol. 230 (1950), pp. 508-511.

ON ARITHMETICAL SUMMATION PROCESSES.*

By AUREL WINTNER.

Part I.

On the Eratosthenian summation process.

Let (C,p), (A), (L) and (E) refer to the summability of Σa_n (where $n=1,2,\cdots$) in the sense of Cesàro, Abel, Lambert and Eratosthenes respectively, the (E)-summability of Σa_n being defined by the existence of $\lim E_n$, where

$$(1)\qquad E_n=E_n(a)=\sum_{k=1}^{n}\{n/k\}a_k \qquad \Bigl(\text{or } E_n=\sum_{k=1}^{\infty}\{n/k\}a_k\Bigr),$$

if $\{x\}$ an abbreviation for $[x]/x$ and $[x]$ denotes the greatest integer not exceeding x (so that the coefficient, $[n/k]k/n$, of a_k in (1) does not exceed 1, and is positive if $1\leqq k\leqq n$). If $a_1,a_2,\cdots$ is replaced by $b_1=b_1(a)$, $b_2=b_2(a),\cdots$, where

$$(2)\qquad b_n=\sum_{d\mid n}a_d/d,$$

then it is readily seen that, for every n,

$$(3)\qquad M_n(b)=E_n(a),$$

where

$$(4)\qquad M_n=M_n(b)=n^{-1}\sum_{k=1}^{n}b_k.$$

An arbitrary assignment of $a_1,a_2,\cdots$ is equivalent to an arbitrary assignment of $b_1,b_2,\cdots$, since the linear substitution (2) has a unique inverse; the explicit form of the latter is

$$(5)\qquad a_n=\sum_{d\mid n}\mu(n/d)b_d/n,$$

where $\mu(k)$ is Möbius' factor. According to (3) and (4), a series Σa_n is (E)-summable if and only if

$$(6)\qquad M(b)=\lim_{n\to\infty}(b_1+\cdots+b_n)/n$$

---

* Received December 14, 1956.

exists, that is, if and only if the series

$$\sum_{n=1}^{\infty} \Delta b_n, \text{ where } \Delta b_n = b_n - b_{n-1}, \qquad (b_0 = 0), \tag{7}$$

is $(C, 1)$-summable.

The replacement of $a_1, a_2, \cdots$ by $E_1, E_2, \cdots$, occurring in particular cases, $a_n = \chi(n)/n$, in the *Disquisitiones Arithmeticae* (and, as a matter of fact, in Euler's writings; for further references, cf. [4], pp. 9-10), was propounded in [4] as a general summation method. First, the following facts were proved in [4], pp. 11-13:

(i) *The convergence of* Σa_n *is neither necessary nor sufficient for the* (E)*-summability of* Σa_n *(but the sum and the* (E)*-sum of* Σa_n *must have the same value when both exist).*

The first of the assertions of (i) can be formulated by saying that the (E)-method is not a regular summation method (in the sense of Toeplitz' criteria). In view of the first and second assertions of (i), there arose the question after appropriate Tauberian restrictions. In this regard, the following criteria were proved in [4], p. 21:

(ii) *The convergence of* Σa_n *is equivalent to the* (E)*-summability of* Σa_n *if any one of the following three conditions is satisfied:*

(I) $|na_n| <$ const.; (II) $a_n \geqq 0$; (III) a_n is lacunary

(by (III) is meant that $a_n = 0$ unless n is in a sequence $m_1, m_2, \cdots$ satisfying $m_{k+1}/m_k >$ const. for some const. > 1).

The prime number theorem follows from that assertion of (ii) which assures that (I) and the (E)-summability of Σa_n together are sufficient for the convergence of Σa_n. In order to see this, it is sufficient to choose $a_n = \mu(n)/n$ and to observe that the (E)-summability of $\Sigma \mu(n)/n$ is trivial (in fact, the case $a_n = \mu(n)/n$ of (5) belongs to $b_1 = 1$, $b_2 = b_3 = \cdots = 0$; so that the numerator of (5) is independent of n, and so the limit (6) certainly exists).

In a subsequent paper, in which [4] is overlooked, Ingham [3] proved a result which refines those assertions of (ii) in which the convergence of Σa_n is the conclusion. In fact, any one of the three conditions (I), (II), (III) is sufficient in order that the $(C, 1)$-simmability, or just the (A)-summability, of Σa_n be equivalent to the convergence of Σa_n (Hardy, Littlewood, Hardy and Littlewood), whereas Ingham's relevant result is as follows:

(iii) *The* (E)*-summability of* Σa_n *is sufficient for the* $(C,1)$*-summability of* Σa_n *(to the same sum).*

Actually, Ingham also shows that the $(C,1)$ in (iii) can be improved to (C,ϵ) if $\epsilon > 0$ (in view of (i), this is not true for $\epsilon = 0$). Incidentally, Theorem (IX_1) in [4], p. 20, is nothing but Theorem 2 in [3], p. 175, since, according to Landau's extension of Hardy's $(C,1)$-lemma, the $(C,1)$-summability and the convergence of Σa_n are equivalent if $a_1 + \cdots + a_n > -\text{const.}$

For reasons explained in [4], I referred to the replacement of the evaluation of Σa_n by means of the sequence $E_1, E_2, \cdots$ as an Eratosthenian summation method. But in the same way as [3], an Appendix to Hardy's posthumous book [1], pp. 376-380, overlooks [4] and renames the (E)-process Ingham's summation process. The oversight is the more curious as Hardy himself wrote the review of [4] in *Nature*, vol. 152 (1943), p. 708.

If

$$M(n) = \sum_{k=1}^{n} \mu(k), \tag{8}$$

then what is involved in the proof of (ii) in [4] as well as in the proof of (iii) in [3] or [1] is something like

$$M(n) = O(n/\log^2 n), \tag{9}$$

an estimate which assures the boundedness of the relevant "Lebesgue constants." This is more than the prime number theorem, which is just

$$M(n) = o(n). \tag{10}$$

But the distinction is less substantial than it was at that time, since, after Selberg, (9) is just as "elementary" as (10). In [3] or [1], the estimate (9) is used directly, and in [4] indirectly, via the theorem of Hardy and Littlewood according to which the (L)-summability of a series is always sufficient for its (A)-summability; cf. [1], pp. 373-374. In fact, something like (9), rather than just (10), is needed in the Hardy-Littlewood proof of $(L) \Rightarrow (A)$. The way in which [4] used $(L) \Rightarrow (A)$ in the proof of (ii) was the following:

The connection (2) between $a_1, a_2, \cdots$ and $b_1, b_2, \cdots$, a connection which, through (3), leads to the formulation (6) of the (E)-summability of Σa_n, is formally equivalent to

$$\sum_{n=1}^{\infty} b_n r^n = \sum_{n=1}^{\infty} n a_n (r^n + r^{2n} + \cdots). \tag{11}$$

It is also clear that the convergence of either of the series (11) for $0 \leqq r < r_0$ implies the convergence of the other series (to the same sum) for $0 < r < r_0$, provided that $0 < r_0 \leqq 1$ (this proviso is satisfied, with $r_0 = 1$, in all the cases considered above). But (11) can be written in the form

$$\sum_{n=1}^{\infty} (\Delta b_n) r^n = (1 - r) \sum_{n=1}^{\infty} n a_n r^n / (1 - r^n), \tag{12}$$

where $\Delta b = b_n - b_{n-1}$ (with $\Delta b_1 = b_1$), and (12) shows that a series $\sum a_n$ is (L)-summable if and only if the corresponding series (7) is (A)-summable (to the same sum).

In what follows, (iii) will be verified, again with the aid of (9), along the lines followed in the proof of (i), that is, by showing that Toeplitz's conditions for a regular process are satisfied by the linear transformation, say

$$S_n = \sum_{m=1}^{n} a_{nm} E_m, \tag{13}$$

where the coefficients a_{nm} are absolute constants and the sequences $E_1, E_2, \cdots$, $S_1, S_2, \cdots$, belonging to an arbitrary series $\sum a_n$, are defined by (1) and

$$(n+1) S_n = \sum_{m=1}^{n} \sum_{k=1}^{m} a_k \tag{14}$$

respectively. The assertion of (iii) is equivalent to

$$\limsup_{n \to \infty} \sum_{m=1}^{n} | a_{nm} | < \infty. \tag{15}$$

In fact, the remaining two of three Toeplitz conditions are

$$\lim_{n \to \infty} \sum_{m=1}^{n} a_{nm} = 1 \tag{16}$$

and

$$\lim_{m \to \infty} a_{nm} = 0 \text{ for } n = 1, 2, \cdots, \tag{17}$$

and both (16) and (17) are trivially satisfied in the present case (cf. below).

First, from (1) where $\{x\} = [x]/x$,

$$n E_n = \sum_{k=1}^{n} [n/k] k a_k; \text{ hence } n E_n = \sum_{m=1}^{n} \sum_{k=1}^{[n/m]} k a_k$$

or, if $T_n = \sum_{k=1}^{n} k a_k$,

$$n E_n = \sum_{m=1}^{n} T_{[n/m]} = \sum_{m=1}^{\infty} T_{[n/m]}$$

$(T_0 = 0)$, and so, by Möbius' inversion,

$$T_n = \sum_{j=1}^{\infty} \mu(j)\,[n/j]E_{[n/j]} = \sum_{j=1}^{n} \mu(j)\,[n/j]E_{[n/j]}.$$

But it follows from (4) that $S_n = \sum_{k=1}^{n} T_k/(k+k^2)$, since $T_k = \sum_{m=1}^{k} m a_m$. Consequently

$$S_n = \sum_{k=1}^{n} (k+k^2)^{-1} \sum_{j=1}^{k} \mu(j)\,[k/j]E_{[k/j]}.$$

If the last relation is thought of as written in the form (13), then it is seen that

$$(18) \qquad a_{nm} = m \sum_{k=1}^{n} (k+k^2)^{-1} \sum_{k/(m+1)<j\leqq k/m} \mu(j).$$

Here the interior sum is $M([k/m]) - M([k/(m+1)])$, by (8). It follows therefore from $(k+k^2)^{-1} < k^{-2}$ that (15) is true if

$$\sum_{k=1}^{n} k^{-2} \sum_{m=1}^{n} m\,|\,M([k/m]) - M([k/(m+1)])\,| < \text{Const.}$$

holds for every n and for some constant. But the existence of such a constant is a straightforward consequence of (9) (if, according to Dirichlet's classical device, the sum is broken into two parts, those contributed by the summation ranges between 1 and $[n^{\frac{1}{2}}]$ and between $[n^{\frac{1}{2}}]+1$ and n).

The four summation processes, mentioned before (1), are "comparable" (in the sense of Hausdorff); their relative position is as follows:

$$(19) \qquad (\mathrm{E}) \Rightarrow (C,1) \Rightarrow (L) \Rightarrow (A).$$

In fact, $(\mathrm{E}) \Rightarrow (C,1)$ is equivalent to (15)-(17), that is, to Ingham's result (iii), and $(L) \Rightarrow (A)$ is the corresponding result of Hardy and Littlewood ([1], Theorem 260), finally $(C,1) \Rightarrow (L)$ is an elementary Abelian lemma of Hardy. The only thing that is peculiar about (E) is that, according to (i),

$$(20) \qquad \text{both } (K) \Rightarrow (\mathrm{E}) \text{ and } (\mathrm{E}) \Rightarrow (K) \text{ are false,}$$

where (K) denotes convergence.

None of the arrows occurring in (19) can be inverted. First, since $(K) \Rightarrow (C,1)$, it is clear from (20) that $(C,1) \Rightarrow (\mathrm{E})$ is false. Next, in order to obtain a series $\sum a_n$ which disproves $(L) \Rightarrow (C,1)$, it is sufficient to choose $a_n = (-1)^n n$, since the corresponding function $\sum a_n z^n$, where $|z| < 1$, remains regular at $z = 1$ but $a_n \neq o(n)$. Finally, the irreversibility of the third arrow in (19) was proved by Hardy and Littlewood [2].

If (E) $\Rightarrow$ (L) is concluded from (19), then there becomes involved the prime number theorem, since the latter is involved in (E) $\Rightarrow$ $(C, 1)$. Actually, the part (E) $\Rightarrow$ (L) of (19) is nothing but Frobenius' $(C, 1)$-variant of Abel's continuity theorem, to be applied to (7). In fact, (3), (4) and (12) show that the $(C, 1)$-summability and the (A)-summability of (7) are equivalent, respectively, to the (E)-summability and the (L)-summability of Σa_n. The latter equivalences, when combined with that theorem of Hardy and Littlewood for which Karamata gave a simple proof, also yield the following Tauberian theorem (which does not involve the prime number theorem):

(†) *The (E)-summability of a (real) series* Σa_n *follows from its (L)-summability if* $\liminf_{n\to\infty} \sum_{d\mid n} a_d > -\infty$.

In fact, the numbers (2) are the partial sums of (7).

Whereas the corollary (E) $\Rightarrow$ (L) of (19) is straightforward, the *weakest* corollary, (E) $\Rightarrow$ (A), of the whole of (19), cannot be proved without the prime number theorem. For it is readily seen from (1) that if $a_n = \mu(n)/n$, then $E_n = 1/n$; hence $\lim E_n = 0$, and so the (E)-summability of Σa_n is now trivial. But if (E) $\Rightarrow$ (A) is granted, then, since $| n a_n | <$ const., the convergence of $\Sigma \mu(n)/n$ follows from Littlewood's (A)-Tauberian theorem.

It is clear from the proof of (15) that the first of the three implications (19) can be refined as follows:

(I) *There exists a universal constant* α *for which* $\operatorname{osc} S_n \leqq \alpha \operatorname{osc} E_n$ *holds whenever* $\limsup | E_n | < \infty$.

Here S_n and E_n are defined, in terms of an arbitrary Σa_n, by (14) and (1) respectively, and $\operatorname{osc} B_n$ denotes the upper limit of $| B_n - B_m |$ as $n > m \to \infty$.

The corresponding refinement of the third of the three implications (19) is equivalent to the following lemma:

(II) *There exists a universal constant* β *for which*

$$\operatorname{osc}(1-r) \sum_{n=1}^{\infty} \Big(\sum_{k=1}^{n} a_k \Big) r^n \leqq \beta \operatorname{osc}(1-r) \sum_{n=1}^{\infty} \Big(\sum_{k\mid n} a_k \Big) r^n \tag{21}$$

holds whenever $\limsup \left| (1-r) \sum_{n=1}^{\infty} \big(\sum_{k\mid n} a_k \big) r^n \right| < \infty$, *with* $\sum_{n=1}^{\infty} | a_n | r^n < \infty$ *for* $0 < r < 1$.

It is understood that $\operatorname{osc} f(r)$ denotes the upper limit of $| f(r) - f(s) |$

as $1 > r > s \to 1$. Hence an inspection of the Hardy-Littlewood proof of $(L) \Rightarrow (A)$ shows that, under the restrictions mentioned after (21),

$$\operatorname{osc} \sum_{n=1}^{\infty} a_n r^n \leqq \beta \operatorname{osc} (1-r) \sum_{n=1}^{\infty} n a_n r^n / (1-r^n) \tag{22}$$

holds for a certain universal β (the theorem of Hardy and Littlewood itself results if the osc on the right of (22) is assumed to be 0). But since the expression on the left of (21) is identical with the left of (22), it is seen from (2) and (11) that (21) is equivalent to the striking assertion of (II).

What is involved in (I) and (II) is (10), and more. I do not know whether (II) could be obtained as an "Abelian" consequence of (I) (somewhat along the lines of Tauber's own theorem, according to which (K) is equivalent to (A) and $T_n = o(n)$ together, where T_n is defined as in the proof of (15) above). Correspondingly, it would be worthwhile to determine the best values of the universal constants α, β occurring in (I), (II), and to decide whether $\alpha < \beta$.

There is a corresponding question concerning an absolute constant which belongs to $(\mathrm{E}) \Rightarrow (L)$ in the same way as α and β belong to $(\mathrm{E}) \Rightarrow (C, 1)$ and $(L) \Rightarrow (A)$ respectively. Actually, the relevant analogue of (I) and (II) is straightforward. It is true that if $(\mathrm{E}) \Rightarrow (L)$ is concluded from (19), then (iii) becomes involved. But this is unnecessary. In fact, it turns out that what corresponds to (I) and (II) is

$$\operatorname{osc} (1-r) \sum_{n=1}^{\infty} n a_n r^n / (1-r^n) \leqq \operatorname{osc} E_n \tag{23}$$

(if $\limsup |E_n| < \infty$), and that the refinement (23) of $(\mathrm{E}) \Rightarrow (L)$ can be reduced to the O-version of Frobenius' Abelian implication $(C, 1) \Rightarrow (A)$. This refinement of $(C, 1) \Rightarrow (A)$, a refinement the truth of which is clear from the proof of $(C, 1) \Rightarrow (A)$, states that

$$\operatorname{osc} \sum_{n=1}^{\infty} a_n r^n \leqq \operatorname{osc} S_n \tag{24}$$

(if $\limsup |S_n| < \infty$). But if the series $\sum a_n$, to which (24) refers, is replaced by the series (7), defined by (2), then it is seen from (3), (4) and (12) that (24) can be written in the form (23).

Since $(C, 1) \Rightarrow (\mathrm{E})$ and $(A) \Rightarrow (L)$ are false, what corresponds to (I) and (II) in the reverse direction is the order of infinity of the "Lebesgue constants." In [4], p. 12, the order of infinity was shown to be logarithmic for the transformation leading from (K) to (E).

Part II.

On Axerian theorems.

A related (but more elementary) arithmetical summation problem which is dealt with in Hardy's posthumous Appendix [1], referred to above, centers about Axer's lemma (cf., e.g., [5], p. 202). In what follows, both types of Axerian facts, presented in [1] (Theorem 267, p. 378) in a form communicated by Ingham, will be improved.

Let $s_1, s_2, \cdots$ be a sequence of numbers satisfying

$$\sum_{n \leqq x} s_n = o(x) \text{ and } s_n = O(1), \tag{25}$$

and let $f(x)$, where $1 \leqq x < \infty$, be a function which is of bounded variation on every *finite* interval,

$$\int_1^x |df(u)| < \infty \text{ if } 1 \leqq x < \infty. \tag{26}$$

By an Axerian condition (*) will be meant a restriction, to be imposed on f alone, to the following effect: Whenever conditions (26) and (*) are satisfied by f, the relation

$$\sum_{n \leqq x} f(x/n) s_n = o(x) \tag{27}$$

holds for every sequence $s_1, s_2, \cdots$ satisfying (25).

Such an Axerian condition (*) is contained in Landau's writings on the "equivalence" questions in the theory of primes (the most delicate of these questions is the deduction of

$$\sum_{n \leqq x} \mu(n)/n = o(1) \text{ from } \psi(x) \sim x, \tag{28}$$

that is, from $\pi(x) \sim x/\log x$). What Landau actually proves is that the existence of a θ satisfying

$$f(x) = O(x^\theta), \text{ where } \theta = \text{const.} < 1, \tag{29}$$

is a (*)-condition (in other words, that (27) follows from (25) whenever (26) and (29) are satisfied by f). In order to obtain (28), it is sufficient to apply (29), with $\theta = \frac{1}{2}$, to the $f(x)$ which represents Dirichlet's remainder term in the divisor problem. Cf. the references in [6], p. 121, and the reproduction of Landau's arguments in [1], pp. 378-380.

In what follows, it will be shown that the Landau's (*)-criterion (29) can be replaced by

$$f(x)=O(\phi(x)), \tag{30}$$

where $\phi(x)$ is any non-negative function satisfying the following conditions:

$$\phi(x) \text{ is monotone} \qquad (\phi \geqq 0) \tag{31}$$

and

$$\int_{1}^{\infty} x^{-2}\phi(x)\,dx<\infty \tag{32}$$

(hence (31) means that $\phi(x)$ is non-increasing). In other words, the following Axerian lemma will be proved:

(*) *If* $f(x)$ *is any function satisfying* (26) *and* (30), *where* $\phi(x)$ *is some function subject to* (31) *and* (32), *then* (27) *is a consequence of* (25).

Remark. In view of (**)) below, it is worth mentioning that the conditions imposed on $f(x)$, $1 \leqq x<\infty$, by (*) can simply be formulated as follows: *If* $g(x)=f(1/x)$, *then*

$$\text{(I)} \quad \int_{+0}^{1} \underset{x \leqq u \leqq 1}{\text{l.u.b.}} |g(u)|\,dx<\infty, \qquad \text{(II)} \quad \int_{x}^{1} |dg(u)|<\infty,$$

where $0<x\leqq 1$ (so that $\int_{+0}^{1} |dg(x)|=\infty$ and $\limsup_{x\to+0} |g(x)|=\infty$ are allowed).

Needless to say, (31) and (32) are satisfied by $\phi(x)=x^{\theta}$ if $0\leqq\theta<1$, that is, when (30) becomes (29). The simplest case in which (29) fails to apply, but the italicized lemma is applicable, results if (30) holds for $\phi(x)=x^2/\log x$. In particular, it follows from (8) and (9) that the following fact is a corollary: *If* $f(x)=\sum_{n\leqq x}\mu(n)$, *then* (27) *holds for any sequence* $s_1, s_2, \cdots$ *satisfying* (25).*

---

* There is a corresponding deduction from Mertens' hypothesis, that is, from

$$\sum_{n\leqq x}\mu(n)=O(\sqrt{x}), \tag{a}$$

as follows: The series

$$\sum_{n=1}^{\infty} s_n\mu(n)/\sqrt{n} \tag{b}$$

is convergent for *every* sequence $s_1, s_2, \cdots$ satisfying

$$s_1\geqq s_2\geqq\cdots \text{ and } \lim s_n=0 \tag{c}$$

if (and only if) Mertens' hypothesis is true.

In fact, (c) and the boundedness of the partial sums of a series Σr_n imply the

The nature of the restrictions imposed on $\phi(x)$ by (31) and (32) is of particular interest, since (31) and (32) are precisely the conditions underlying a theorem of Landau (Satz 3 in [6], pp. 123-124), a theorem which applies in a direction just the opposite to the direction of an Axerian implication (and *assumes*, therefore, the prime number theorem; in this regard, cf. Ingham's Theorems 1 and 3 in [3]).

The proof of the italicized criterion (*) will depend on the following elementary lemma: If $h(t)$ is any function which is monotone on the open half-line $0 < t < \infty$ and is integrable on its closure (in the sense that both

$$(31') \qquad \lim_{\epsilon \to 0} \int_{\epsilon}^{1} h(t)\,dt \text{ and } \lim_{\epsilon \to 0} \int_{1}^{1/\epsilon} h(t)\,dt$$

exist), then, as $x \to \infty$,

$$(32') \qquad \sum_{n=1}^{\infty} h(n/x) \sim Cx, \text{ where } C = \int_{+0}^{\infty} h(t)\,dt$$

(the convergence of the series (32′) for any fixed $x > 0$ is part of the statement). The fact that the monotony of $h(t)$ on $0 < t < \infty$ and the finiteness of both integrals (31′) imply (32′), is just a restatement of no. 30 in chap. II of [7].

Starting with a function $\phi(x)$ on the closed half-line $1 \leqq x < \infty$ and assuming (31) and (32), define on the open half-line $0 < t < \infty$ a function $h(t)$ by placing $h(t) = \phi(1/t)$ if $0 < t \leqq 1$ and $h(t) = 0$ if $1 < t < \infty$. Then it is clear that the conditions required of h in (32′), the convergence of both integrals (31′) and the monotony of h, are satisfied. Hence it is also clear that the same conditions remain satisfied if any positive $\epsilon < 1$ is chosen and if the preceding $h(t)$ is replaced by the function $h_\epsilon(t)$ which is

---

convergence of the series $\Sigma r_n s_n$ (Abel-Dedekind). Hence, if the latter series is identified with (b), the convergence of (b) follows from the assumptions (c) if

$$\text{(d)} \qquad \sum_{n \leqq x} \mu(n)/\sqrt{n} = O(1)$$

is true. But while a partial summation leads from (d) to (a), it is clear that (a) *in itself* fails to imply (d). It was however shown in [8] that, for *function-theoretical* Tauberian reasons, (d) must be true if (a) is true. Accordingly, (a) would be disproved if one could construct a *single* sequence $s_1, s_2, \cdots$ satisfying the conditions (c) and rendering the series (b) divergent.

Conversely, if there does not exist such a sequence, then (d), hence (a), is true. For, according to Hadamard's converse of the elementary lemma used above (Abel-Dedekind), the partial sums of a series Σr_n must be bounded if the series $\Sigma r_n s_n$ is convergent for *every* sequence $s_1, s_2, \cdots$ satisfying (c).

identical with the preceding $h(t)$ for $0 < t \leqq \epsilon$ and is 0 for $\epsilon < t < \infty$. Accordingly, (32′) is valid if $h(t)$ is replaced by $h_\epsilon(t)$. But then, since

$$\sum_{n=1}^{\infty} h_\epsilon(n/x) = \sum_{n \leqq \epsilon x} h_\epsilon(n/x) = \sum_{n \leqq \epsilon x} \phi(x/n),$$

(32′) reduces to $\sum_{n \leqq \epsilon x} \phi(x/n) \sim x \int_{+0}^{\infty} h_\epsilon(t)\,dt$, where ϵ is fixed $(0 < \epsilon < 1)$ and $x \rightarrow \infty$. But

$$\int_{+0}^{\infty} h_\epsilon(t)\,dt = \int_{+0}^{\epsilon} \phi(1/t)\,dt = \int_{1/\epsilon}^{\infty} u^{-2} \phi(u)\,du$$

(where $u = 1/t$), and the last integral tends to 0 as $\epsilon \rightarrow 0$, since (32) is assumed (and $\phi \geqq 0$). Consequently

$$\lim_{\epsilon \rightarrow 0} \lim_{x \rightarrow \infty} x^{-1} \sum_{n \leqq x} \phi(x/n) = 0, \tag{33}$$

where the existence of the interior lim (for fixed ϵ) and of the repeated limit are parts of the conclusion.

If the interior lim is replaced by lim sup, then it is clear from (30), where $\phi \geqq 0$, that ϕ can be replaced by $|f|$ in (33). It follows therefore from the second of the two assumptions (25) that

$$\lim_{\epsilon \rightarrow 0} \lim_{x \rightarrow \infty} x^{-1} \Big| \sum_{n \leqq \epsilon x} f(x/n) s_n \Big| = 0. \tag{34}$$

Note that neither (26) nor the first of the two assumptions (25) was used thus far.

The relation (34) turns out to be the main point in the proof of the assertion, (27), of (*). In fact, owing to (34), the balance of the proof of (27) becomes the same as it is under Landau's assumption (29). In fact, (35) takes the place of the third formula line in [1], p. 379, and the balance of the proof (p. 379, lines 1-10, in [1], where the delta is the present epsilon) can be repeated *verbatim*. Suffice it to say that the partial summation and its estimate, carried out in [1] on the second half of p. 379, involve nothing like (29) or (30) above, but merely (26) and (25). The proof of (*) is therefore complete.

Axer's own result (for references, cf. [6], p. 121) weakens the second of the two assumptions (25) so as to replace (25) by

$$\sum_{n \leqq x} s_n = o(x) \text{ and } \sum_{n \leqq x} |s_n| = O(x), \tag{35}$$

and it states that (35) is sufficient for the truth of (27) if $f(x)$ is chosen as follows:

$$f(x) = x - [x] \text{ for } 1 \leqq x < \infty. \tag{36}$$

In Ingham's approach to the Axerian lemmas (Theorem 267 in [1]), the assumptions (25) and (35) are treated simultaneously (by a partial summation) and, correspondingly, it is proved that (27) can be concluded from (35) when (36) is generalized to any *bounded* function $f(x)$ satisfying (26).

It turns out however that, precisely under the assumption (35), the method of partial summations, which involves (26), is quite misleading. In fact, the true generalization of (36) (in the case (35)) has nothing to do with the assumption (26) of (*), since the true condition on $f(x)$, where $1 \leqq x < \infty$, is simply the following: If $g(x)$ is defined by

$$g(x) = f(1/x) \text{ if } 0 < x \leqq 1 \text{ and } g(x) = g(0) \text{ if } x = 0 \tag{37}$$

then

$$g(x) \text{ is } R\text{-integrable on } 0 \leqq x \leqq 1. \tag{38}$$

In contrast, what Ingham's result (quoted in the preceding section) requires is that $g(x)$ be bounded* on $0 < x \leqq 1$ and of bounded variation on $\epsilon \leqq x \leqq 1$ if $0 < \epsilon < 1$. Actually, that (38) alone is enough is clear from 4, p. 2, where a very short proof is given for Axer's own case, (36). In fact, a glance at that proof shows that only (38) is needed:

(**) *If $f(x)$, where $1 \leqq x < \infty$, is any function corresponding to which the condition* (38) *is satisfied by the function $g(x)$ defined for $0 \leqq x \leqq 1$ by* (37), *then* (27) *is a consequence of* (35).

It is seen from (37) that (27) can be written in the form

$$\sum_{n \leqq x} g(n/x) = o(x) \tag{39}$$

(the value $g(0)$, assigned in (37) in order to render (38) meaningful, is immaterial). On the other hand, if x is replaced by ax and bx in the first of the assumptions (37), it follows, by subtraction, that

$$\sum_{a < x \leqq b} s_n = o(x) \tag{40}$$

---

* This is *implied* by (38). Originally (in Riemann's own paper and, until comparatively recently, in all books) the boundedness was an explicit *additional* condition of R-integrability. Actually the redundancy of this proviso, usually attributed to Landau's *Einführung in die Differentialrechnung und Integralrechnung* (1934), was recognized already by Hölder, on p. 3 of his *Beiträge zur Potentialtheorie* (Tübingen dissertation, Stuttgart, 1882).

whenever $0 \leqq a < b \leqq 1$. But (40) means that (39) is true for the function $g(x)$ which is 1 or 0 according as x is or is not on the subinterval $a < x \leqq b$ of $0 \leqq x \leqq 1$. Thus, for reasons of distributivity, (39) is true whenever $g(x)$ is a step-function (with a finite number of jumps) on $0 \leqq x \leqq 1$. Hence it is seen from the second of the assumptions (35), which was not used thus far, that (39) is true whenever $g(x)$ has the following property: There belongs to every $\epsilon > 0$ a pair of step-functions $g_\epsilon(x)$, $g^\epsilon(x)$ in such a way that, on the one hand, $g_\epsilon \leqq g \leqq g^\epsilon$ for $0 \leqq x \leqq 1$ and, on the other hand, the integral of $g^\epsilon - g_\epsilon$ (over $0 \leqq x \leqq 1$) is less than ϵ. Since the existence of such a pair g_ϵ, g^ϵ (for every $\epsilon > 0$) is equivalent to (38), the proof of (**) is complete.

Appendix.

Let Σa_n, where $n = 1, 2, \cdots$, be a series satisfying $\limsup |a_n|^{1/n} \leqq 1$. This means that the power series $f(x) = \Sigma a_n e^{-nx}$, where $f(\infty) = a_0 = 0$, converges for $x > 0$, and $f(x) = O(e^{-x})$ as $x \to \infty$, where $f' = df/dx$. Let the additional hypotheses requiring the convergence (at $x = +0$) of the integrals

$$\int_0^\infty f'(x)\,dx, \quad \int_0^\infty |f'(x)|\,dx, \quad \int_0^\infty \phi(x)\,dx, \text{ where } \phi(x) = \underset{x \leqq y < \infty}{\text{l. u. b.}} |f'(y)|,$$

(and, in all three cases, $\int_0^\infty = \int_{+0}^\infty$) be referred to by A, $|A|$, $\|A\|$ respectively. Thus A means the (A)-summability (Abel), and $|A|$ the absolute (A)-summability (J. M. Whittaker), of Σa_n, and $\|A\|$ requires more than $|A|$. Suffice it to say that, while $|A|$ is compatible with $\limsup x\,|f'(x)| = \infty$, where $x \to 0$, it follows from $\|A\|$ that $xf'(x) \to 0$, since the *monotony* and the integrability (at $x = +0$) of $\phi(x)$ imply that $x\phi(x) \to 0$.

A theorem of Ananda-Rau [9] states that *the* $\|A\|$*-summability of* Σa_n *implies the* (L)*-summability of* Σa_n. For this theorem of Ananda-Rau, whose proof is quite involved, Hardy and Littlewood [2], p. 259, gave a shorter proof which, however, a note in Hardy's book [1], p. 376, recognizes to be fallacious. By claiming a generalization of Ananda Rau's theorem, I committed a corresponding blunder in [10], p. 686, assertion (β_0). Since the sufficiency of $\|A\|$-summability for L-summability is just stated, but not proved, in Hardy's book [1], p. 376 (Theorem 263), the only correct proof available in the literature appears to be Ananda-Rau's complicated approach [9].

It turns out, however, that Ananda-Rau's theorem follows in an almost trivial fashion if recourse is had to the simple device used at the beginning of the proof of (*) above. In order to see this, the following lemma (§), which has nothing to do with questions of summability, will first be isolated.

(§) *Let* $F(x)$, *where* $0 < x < \infty$, *be a function which is R-integrable on every interval* $\lambda \leqq x \leqq \mu$, *where* $0 < \lambda < \mu < \infty$, *and suppose that there exists a monotone function* $\phi(x)$ *satisfying* $|F(x)| \leqq \phi(x)$ *and having a finite (improper) integral over* $0 < x < \infty$. *Then*

$$h \sum_{n=1}^{\infty} F(nh) \rightarrow \int_{0}^{\infty} F(x)dx \text{ as } h \rightarrow +0 \qquad \left(\int_{0}^{\infty} = \int_{+0}^{1} + \int_{1}^{\infty}\right)$$

(*and* $\sum_{n=1}^{\infty} F(nh)$ *is absolutely convergent for every* $h > 0$).

First, if F is monotone throughout (so that either F or $-F$ can be chosen to be ϕ), then the assertion of (§) becomes the straightforward fact referred to at the beginning of the proof of (*) above ([7], chap. II, no. 30). Next, if F satisfies only the assumptions made in (§), then, by the proof of (*) above,

$$\lim_{\lambda \rightarrow 0} \limsup_{h \rightarrow 0} |h \sum_{n \leqq \lambda h} F(nh)| = 0,$$

since $\phi(x)$ is a montone and integrable majorant of $|F(x)|$ near $x = +0$. But if $x = +0$ is replaced by $x = \infty$, then the same argument shows that

$$\lim_{\mu \rightarrow \infty} \limsup_{h \rightarrow 0} |h \sum_{n \geqq \mu h} F(nh)| = 0.$$

Finally, since $F(x)$ is supposed to be R-integrable on every interval $\lambda \leqq x \leqq \mu$, where $0 < \lambda < \mu < \infty$, it is clear that, when λ (> 0) and μ $(> \lambda)$ are fixed,

$$h \sum_{\lambda h < n < \mu h} F(nh) \rightarrow \int_{\lambda}^{\mu} F(x)dx \text{ as } h \rightarrow 0.$$

Clearly, the assertion of (§) follows from the last three formula lines (by adding three epsilons).

In order to obtain Ananda-Rau's theorem as a corollary of (§), suppose that $\sum a_n$ is $\| A \|$-summable. By definition, this means that the assumptions of (§) are satisfied by $F(x) = f'(x)$, where $f(x) = \Sigma a_n e^{-nx}$ and $f' = df/dx$. Hence, if h is replaced by x in the assertion of (§),

$$\lim_{x \to 0} x \sum_{n=1}^{\infty} f'(nx) = \int_{+0}^{\infty} f'(x)dx = f(\infty) - f(+0) = -f(+0)$$

(the last integral is [absolutely] convergent, since $\| A \|$-summability clearly implies [absolute (A)-summability, hence] (A)-summability, that is, the existence of $f(+0)$, whereas $f(\infty) = 0$ is obvious from $f'(x) = O(e^{-x})$ as $x \to \infty$). On the other hand, it is clear that, if $0 < x < \infty$,

$$\sum_{n=1}^{\infty} f'(nx) = -g(x), \text{ where } g(x) = \sum_{n=1}^{\infty} na_n e^{-nx}/(1 - e^{-nx})$$

(simply because $f(x) = \Sigma a_n e^{-nx}$, hence $f'(x) = -\Sigma na_n e^{-nx}$). But the last two formula lines show that $-xg(x) \to -f(+0)$ as $x \to +0$, which, in view of the definition of $g(x)$, proves that Σa_n is (L)-summable (to the same sum, $f(+0)$, as under (A)-summability).

Clearly, the ϕ-assumption imposed on $F(x)$ in (§) plays the part of a Tauberian restriction. There are other such restrictions which are sufficient for the truth of the assertion of (§). For the sake of simplicity, such a criterion will now be formulated for $0 < x \leqq 1$ (rather than, as in (§), for $0 < x < \infty$), as follows:

(§§) *If* $F(x)$, *where*, $0 < x \leqq 1$, *is a real-valued function which has a continuous derivative* $F'(x)$ *satisfying the Tauberian restriction*

$$\liminf_{x \to 0} x^2 F'(x) > -\infty,$$

then

$$h \sum_{n=1}^{[1/h]} F(nh) \to \int_{+0}^{1} F(x)dx \text{ as } h \to 0$$

whenever the improper integral of $F(x)$ *exists* (*it need not converge absolutely*).

In fact, if the preceding reduction of Ananda-Rau's theorem to (§) is compared with the proof of that criterion of Hardy and Littlewood on (L)-summability which is Theorem 262 in [1], then it becomes clear that the proof of (§§) is contained between the lines of [1], pp. 375-376. In the particular case of Hardy and Littlewood, the $F(x)$ of (§§) becomes the first derivative of $f(x) = \Sigma a_n e^{-nx}$ (so that the Tauberian restriction of (§§) leads to f'').

Needless to say, the existence of continuous $F'(x)$ is used in the proof of (§§) only in the immediate vicinity of $x = +0$ (for $\epsilon \leqq x \leqq 1$, where $0 < \epsilon < 1$, the R-integrability of $F(x)$ is more than sufficient). In addition, the continuity of the derivative can readily be dispensed with.

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

Part I.

[1] G. H. Hardy, *Divergent Series*, Oxford, 1949.

[2] G. H. Hardy and J. E. Littlewood, "Notes on the theory of series (XX): on Lambert series," *Proceedings of the London Mathematical Society*, vol. 41 (1936), pp. 257-270.

[3] A. E. Ingham, "Some Tauberian theorems connected with the prime number theorem," *Journal of the London Mathematical Society*, vol. 20 (1945), pp. 171-180.

[4] A. Wintner, *Eratosthenian Averages*, Baltimore, 1943.

Part II.

[5] E. Hecke, *Theorie der algebraischen Zahlen*, Leipzig, 1923.

[6] E. Landau, Über einige neuere Grenzwertsätze, *Rendiconti del Circolo Matematico di Palermo*, vol. 34 (1912), pp. 121-131.

[7] G. Pólya and G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, vol. 1, Berlin, 1925.

[8] A. Wintner, "A note on Mertens' hypothesis," *Revista de Ciencias*, (Lima) Ano L, 1949, pp. 181-184.

Appendix.

[9] K. Ananada-Rau, "On Lambert's series," *Proceedings of the London Mathematical Society*, vol. 19 (1921), pp. 1-20.

[10] A. Wintner, "The sum formula of Euler-Maclaurin and the inversions of Fourier and Möbius," *American Journal of Mathematics*, vol. 69 (1947), pp. 685-708.

POSITIVITÄTSBEREICHE IM R^n.*

Von Max Koecher.

1. **Einleitung.** In der vorliegenden Untersuchung werden gewisse Kegelbereiche des n-dimensionalen reellen Zahlenraumes—Positivitätsbereiche genannt—durch drei einfache Eigenschaften definiert und diese Bereiche dann systematisch untersucht. Aus den relativ schwachen Forderungen, die an diese Bereiche gestellt werden, können eine Reihe von teilweise überraschenden Eigenschaften abgeleitet werden, die bisher nur in Spezialfällen bekannt waren. Es soll dies hier an einem Beispiel erläutert werden.

Das einfachste nicht-triviale Beispiel von Positivitätsbereichen geben diejenigen symmetrischen Matrizen, die als Matrix einer positiv definiten quadratischen Form fester Variablenzahl aufgefasst werden können. Prozesse wie z. B. die Bildung der Determinante oder der inversen Matrix und die Konstruktion einer beim Übergang zu äquivalenten Matrizen invarianten Massbestimmung lassen sich auch in den allgemeinen Positivitätsbereichen durchführen. Damit ergeben sich Beispiele von Bereichen, die ähnlich einfache Eigenschaften wie die quadratischen Formen besitzen.

Es zeigt sich, dass für Positivitätsbereiche eine gemeinsame Zahlentheorie (in Analogie zu der der quadratischen Formen) entwickelt werden kann. Darüber soll jedoch an anderer Stelle berichtet werden.

In der Darstellung des Stoffes wurde so vorgegangen, dass zuerst im Abschnitt **2** Positivitätsbereiche in topologischen Vektorräumen mit Norm definiert werden und für diese eine Reihe von einfachsten Eigenschaften abgeleitet werden. Ab Abschnitt **3** tritt jedoch eine Beschränkung auf den n-dimensionalen Zahlenraum ein. An manchen Stellen mögliche Verallgemeinerungen wurden dabei ausser acht gelassen. Bei der Lektüre ist zu empfehlen, sich an den Beispielen in **11** zu orientieren.

2. **Positivitätsbereiche in topologischen Vektorräumen.** Es sei R der mit der natürlichen Topologie versehene Körper der reellen Zahlen und X ein Vektorraum über R. Wir setzen voraus, dass X eine Norm zulässt, d. h. es existiert eine Abbildung $x \to |x|$ von X in R^+ mit den folgenden Eigenschaften:

---

* Received March 9, 1957.

$$|x| = 0 \text{ ist äquivalent mit } x = 0,$$
$$|\lambda x| = |\lambda| \cdot |x| \text{ für alle } \lambda \text{ aus } R \text{ und } x \text{ aus } X,$$
$$|x + y| \leqq |x| + |y| \text{ für alle } x \text{ und } y \text{ aus } X.$$

Diese Norm definiert auf X eine Topologie und in dieser Topologie wird X zu einem topologischen Vektorraum über R.

Eine Abbildung $L(a,b)$ von $X \times X$ in R nennen wir zur Abkürzung eine *Bilinearform von X*, wenn gilt:

(B.1) $L(a,b) = L(b,a)$ für alle a und b aus X,

(B.2) $L(a,x)$ ist bei festem a in x linear und stetig.

Für eine solche Bilinearform L bezeichnen wir mit $X(L)$ die Menge der a aus X mit $L(a,x) = 0$ für alle x aus X. Wegen $L(0,x) = 0$, x aus X, ist $X(L)$ sicher nicht leer. Man sieht ausserdem sofort, dass $X(L)$ ein in X enthaltener topologischer Vektorraum über R ist. Eine Bilinearform L von X heisse *ausgeartet*, wenn $X(L)$ nicht nur aus der Null besteht.

Ist L eine Bilinearform von X, dann nennen wir eine Teilmenge Y von X einen *Positivitätsbereich von X mit L als Charakteristik*, wenn gilt:

(P.0) Y ist offen und nicht leer.

(P.1) Für alle a und b aus Y gilt $L(a,b) > 0$.

(P.2) Liegt x nicht in Y, dann gibt es ein a aus $\bar{Y}$, welches nicht zu $X(L)$ gehört, mit $L(a,x) \leqq 0$.[1]

Man wird später an Beispielen sehen, dass L keineswegs durch die Punktmenge Y eindeutig bestimmt ist. Eine Punktmenge Y von X heist ein *Positivitätsbereich von X* schlechthin, wenn es eine Bilinearform L von X derart gibt, dass Y ein Positivitätsbereich von X mit L als Charakteristik wird. (P.1) zeigt sofort, dass jede Charakteristik eines Positivitätsbereiches nicht identisch Null ist.

Offenbar sind die Axiome (P.1) bzw. (P.2) von den Axiomen (P.0), (P.2) bzw. (P.0), (P.1) unabhängig. Dass aber auch (P.0) von (P.1), (P.2) unabhängig ist, zeigt das einfache Beispiel

$$X = R^2, Y = \{y : y = \begin{pmatrix} y^1 \\ y^2 \end{pmatrix}, \ y^1 \geqq 0, y^2 > 0\},$$

wenn man als Bilinearform das Skalarprodukt zweier Vektoren nimmt.

---

[1] Wie üblich wird für Teilmengen A von X mit $\bar{A}$ die abgeschlossene Hülle und mit $\mathring{A}$ der offene Kern von A bezeichnet und $Rd(A) = \bar{A} - \mathring{A}$ gesetzt.

SATZ 1. *Für jeden Positivitätsbereich Y von X gilt:*

a) *Für jede Charakteristik L von Y und jedes a aus $\bar{Y}$, welches nicht in $X(L)$ liegt, ist $L(a,y) > 0$ für alle y aus Y.*

b) *Mit a und b liegt auch $a+b$ in Y.*

c) *Mit a liegt auch λa in Y, falls $\lambda > 0$.*[2]

d) *Liegt x nicht in $\bar{Y}$, dann gibt es a aus Y mit $L(a,x) < 0$.*

e) *Liegen a und $-a$ in $\bar{Y}$, dann gehört a für jede Charakteristik L zu $X(L)$.*

Beweis: a) Wegen (P.1) kann man annehmen, dass a ein Punkt von $Rd(Y)$ ist. Man hat dann $L(a,y) \geqq 0$ für alle y aus Y. Nehmen wir jetzt an, dass $L(a,y) = 0$ für ein y aus Y erfüllt wäre. Da Y offen ist, gibt es zu jedem x aus X ein $\lambda > 0$, für das $y + \lambda x$ in Y liegt. Jetzt hat man

$$0 \leqq L(a, y+\lambda x) = L(a,y) + \lambda L(a,x) = \lambda L(a,x),$$

d.h. $L(a,x) \geqq 0$ für alle x aus X. Da mit x auch $-x$ zu X gehört, folgt $L(a,x) = 0$, d.h. a liegt in $X(L)$.

b) Würde für a und b aus Y der Punkt $a+b$ nicht in Y liegen, dann gibt es nach (P.2) ein c aus $\bar{Y}$ mit

$$0 \geqq L(c, a+b) = L(c,a) + L(c,b)$$

und c nicht aus $X(L)$. Das ist aber ein Widerspruch, denn nach a) gilt $L(c,a) > 0$ und $L(c,b) > 0$.

c) Die Behauptung kann analog zu b) erschlossen werden.

d) Wir nehmen an, dass für ein x, welches nicht in $\bar{Y}$ liegt, die Behauptung falsch ist, d.h. es gilt $L(a,x) \geqq 0$ für alle a aus Y. Da das Komplement von $\bar{Y}$ sicher offen ist, können wir zu gegebenen c aus Y ein $\lambda > 0$ so bestimmen, dass auch $x + \lambda c$ nicht in $\bar{Y}$ liegt. Jetzt folgt für alle a aus Y nach (P.1)

$$L(a, x+\lambda c) \geqq \lambda L(a,c) > 0$$

oder

$$L(a, x+\lambda c) \geqq 0 \text{ für alle } a \text{ aus } \bar{Y}.$$

Andererseits gibt es nach (P.2) ein a aus $\bar{Y}$, welches nicht in $X(L)$ liegt, mit $L(a, x+\lambda c) \leqq 0$, d.h.

$$0 = L(a, x+\lambda c) = L(a,x) + \lambda L(a,c).$$

---

[2] Kleine griechische Buchstaben bezeichnen stets reelle Zahlen.

Da aber $L(a,x)$ und $L(a,c)$ nicht negativ sind, folgt $L(a,c)=0$ im Widerspruch zu a).

e) Nach (P.1) hat man sofort $L(a,y)\geqq 0$ und $L(-a,y)\geqq 0$ für alle y aus Y, d.h. $L(a,y)=0$. Zu jedem x aus X bestimmen wir nun wieder $\lambda>0$ derart, dass $y+\lambda x$ in Y liegt und erhalten

$$0=L(a,y+\lambda x)=L(a,y)+\lambda L(a,x)=\lambda L(a,x).$$

x ist also Punkt von $X(L)$ und der Satz ist vollständig bewiesen.

Als einfache Folge dieses Satzes ergibt sich, dass $X(L)$ für jede Charakteristik L von Y eine Teilmenge von $Rd(Y)$ ist. Denn ein Punkt a von $X(L)$ gehört wegen (P.1) nicht zu Y und wegen Satz 1d sicher zu $\bar{Y}$.

Die Positivitätsbereiche von topologischen Vektorräumen sind maximal, man überlegt sich nämlich sofort, dass für zwei Positivitätsbereiche Y und $\tilde{Y}$ von X mit gleicher Charakteristik aus $Y\subseteq\tilde{Y}$ stets $Y=\tilde{Y}$ folgt.

Ein Positivitätsbereich Y möge *ausgeartet* genannt werden, wenn Y eine ausgeartete Charakteristik besitzt.

SATZ 2. *Sei Y ein Positivitätsbereich von X.*

a) *Ist X direkte Summe zweier Vektorräume $\tilde{X}$ und X_0, $X=\tilde{X}\oplus X_0$, und gilt gleichzeitig eine Zerlegung $Y=\tilde{Y}\oplus X_0$, dann ist jede Charakteristik von Y ausgeartet.*

b) *Ist Y ausgeartet, dann gibt es eine Zerlegung $X=\tilde{X}\oplus X_0$ von X in zwei topologische Vektorräume, hierbei ist ausserdem $Y=\tilde{Y}\oplus X_0$ und $\tilde{Y}$ ist Positivitätsbereich von $\tilde{X}$.*

Beweis: a) Sei L eine Charakteristik von Y und $x=\tilde{x}+x_0$ die direkte Zerlegung des allgemeinen Punktes von X. Sind a und y jetzt zwei Punkte von Y in der gleichen Zerlegung, dann folgt nach (P.1)

$$0<L(a,y)=L(\tilde{a},\tilde{y})+L(\tilde{a},y_0)+L(a_0,\tilde{y})+L(a_0,y_0).$$

Für $a_0\to 0$ und $\tilde{y}\to 0$ hat man

$$L(\tilde{a},y_0)\geqq 0 \text{ für alle } \tilde{a} \text{ aus } \tilde{Y} \text{ und } y_0 \text{ aus } X_0,$$

und $\tilde{a}\to 0$, $\tilde{y}\to 0$ liefert entsprechend

$$L(a_0,y_0)\geqq 0 \text{ für alle } a_0 \text{ und } y_0 \text{ aus } X_0.$$

Zusammen ist also $L(a,y_0)\geqq 0$, d.h.

$$L(a,y_0)=0 \text{ für alle } a \text{ aus } Y \text{ und } y_0 \text{ aus } X_0.$$

Wie im Beweis zu Satz 1e folgt hieraus, dass dies sogar für alle a aus X richtig ist, d.h. X_0 ist Teilmenge von $X(L)$ und L ist sicher ausgeartet.

b) Wir zeigen zuerst, dass X in eine direkte Summe zerlegt werden kann. Wir wählen dazu ein c mit $|c| = 1$ aus $X(L)$, setzen $X_0 = \{\lambda c\}$ und definieren für x_0 aus X_0

$$M(x_0) = \lambda, \text{ falls } x_0 = \lambda c.$$

$M(x)$ ist dann eine auf X_0 definierte stetige Linearform, die nach dem Satz von Hahn-Banach auf ganz X als stetige Linearform fortgesetzt werden kann. Für x aus X setzt man

$$\tilde{x} = x - M(x) \cdot c, \qquad x_0 = M(x)c$$

Die Zerlegung $x = \tilde{x} \oplus x_0$ ist dann direkt und es gilt $M(\tilde{x}) = 0$. Man erhält also eine Zerlegung von X in eine direkte Summe zweier Vektorräume $\tilde{X}$ und X_0. Da X_0 von c aufgespannt wird, ist stets

$$L(a,x) = L(a,\tilde{x}) = L(\tilde{a},\tilde{x}).$$

Wir setzen jetzt $\tilde{Y} = Y \cap \tilde{X}$ und zeigen, dass $\tilde{Y}$ Positivitätsbereich von $\tilde{X}$ mit $L(a,b)$ als Charakteristik ist. Zum Beweis dieser Behauptung ist zuerst (P.0) trivial. Für (P.1) seien $\tilde{a}$ und $\tilde{b}$ Punkte aus $\tilde{Y}$, dann gehören sie auch zu Y und man hat $L(\tilde{a},\tilde{b}) > 0$. Ist andererseits $\tilde{x}$ nicht aus $\tilde{Y}$, dann liegt $\tilde{x}$ auch nicht in Y. Nach (P.2) gibt es a aus $\tilde{Y}$, welches nicht in $X(L)$ liegt, mit $0 \geqq L(a,\tilde{x}) = L(\tilde{a},\tilde{x})$ und $\tilde{a}$ ist natürlich in $\overline{\tilde{Y}}$ enthalten. Damit ist aber auch (P.2) für $\tilde{Y}$ nachgewiesen. Zum vollständigen Beweis der Behauptung fehlt noch der Nachweis von $Y = \tilde{Y} \oplus X_0$. Wie vorher überlegt man sich sofort, dass $\tilde{Y} \oplus X_0$ ein Positivitätsbereich mit L als Charakteristik ist und $Y \supseteq \tilde{Y} \oplus X_0$ gilt. Wegen der Maximalität der Positivitätsbereiche folgt daraus die Gleichheit.

Nach diesem Satz kann man die Positivitätsbereiche in einfacher Weise auf nicht ausgeartete Positivitätsbereiche zurückführen und man übersieht alle Positivitätsbereiche, wenn man die nicht ausgearteten kennt.

Ist Y ein nicht ausgearteter Positivitätsbereich von X, dann kann man für die Punkte von X eine Relation "$\geqq$" (bzw. "$>$") durch

$$x \geqq y \text{ ist äquivalent mit } x - y \in \bar{Y}$$

$$(\text{bzw. } x > y \text{ ist äquivalent mit } x - y \in Y)$$

definieren. Diese Relation induziert dann in X eine *Halbordnung*, die mit R verträglich ist, d.h. es gilt:

Aus $x \geqq y$ und $y \geqq z$ folgt $x \geqq z$.

Aus $x \geqq y$ und $y \geqq x$ folgt $x = y$.

Aus $x \geqq y$ folgt $a + x \geqq a + y$.

Aus $x \geqq y$ und $0 < \lambda \in R$ folgt $\lambda x \geqq \lambda y$.

Wir werden in Zukunft bei nicht ausgearteten Positivitätsbereichen für deren Punkte y auch $y > 0$ schreiben. Für a und b aus X und y aus Y hat man $L(a, y) > L(b, y)$ wenn $a > b$, d. h. die Bilinearform ist monoton.

3. Positivitätsbereiche im R^n. Von nun an werden wir nur endlichdimensionale Vektorräume zu betrachten haben und können uns daher auf den Fall $X = R^n$ beschränken. Die Punkte x des R^n schreiben wir als *Spalten*

$$x = \begin{pmatrix} x^1 \\ x^2 \\ \cdot \\ \cdot \\ \cdot \\ x^n \end{pmatrix}, x' = (x^1, x^2, \cdots, x^n)$$

und benützen konsequent den Matrizenkalkül. Als Norm des R^n nehmen wir $|x| = (x'x)^{\frac{1}{2}}$. Eine Bilinearform $L(a, b)$ des R^n hat dann die Form $L(a, b) = a'Sb = b'Sa$ mit einer geeigneten reellen symmetrischen n-reihigen Matrix S. Wir wollen jetzt auch S eine Charakteristik von Y nennen, wenn dies für $L(a, b)$ der Fall ist. $L(a, b)$ ist genau dann ausgeartet, wenn $|S| = 0$. Aus Satz 2 folgt, dass such jeder ausgeartete Positivitätsbereich Y in der Form $Y = \bar{Y} \oplus R^q$ $(0 < q < n)$ schreiben lässt, wobei $\bar{Y}$ ein geeigneter Positivitätsbereich des R^{n-q} ist. Man erkennt hieraus, dass durch Y der Rang der Charakteristik S eindeutig bestimmt ist.

Für reelle Matrix W von n Zeilen und Spalten und Punktmenge A des R^n möge mit WA die Menge der Bildpunkte von A bei der Abbildung $y \to Wy$ bezeichnet werden. Es ist dann sofort zu sehen, dass mit Y auch WY, $|W| \neq 0$, ein Positivitätsbereich ist. Ist hier S eine Charakteristik von Y, dann ist $W'^{-1}SW^{-1}$ eine Charakteristik von WY.

Ist Y ein Positivitätsbereich des R^n, S eine Charakteristik von Y, dann kann man als Ergänzung zu Satz 1 zeigen, dass zu jedem a aus $Rd(Y)$ ein b aus $Rd(Y)$ mit $Sb \neq 0$ und $a'Sb = 0$ existiert. Sei dazu a_ν eine gegen a konvergente Folge, deren Glieder nicht aus $\bar{Y}$ gewählt sind. Nach Satz 1d gibt es dann b_ν aus Y mit $a'_\nu Sb_\nu < 0$. Man kann hier noch ohne Einschränkung $|Sb_\nu| = 1$ annehmen. Wir wählen nun eine Teilfolge der a_ν derart, dass die zugehörigen b_ν gegen einen Punkt b von $\bar{Y}$ konvergieren. Man hat dann $a'Sb \leqq 0$, $|Sb| = 1$. Nach (P. 1) ist aber nur $a'Sb = 0$ möglich.

4. Nicht ausgeartete Positivitätsbereiche des R^n. Da man sich nach den Überlegungen in **2** und **3** bei den weiteren Untersuchungen auf nicht ausgeartete Positivitätsbereicche beschränken kann, wollen wir von nun an stets annehmen, dass Y ein nicht ausgearteter Positivitätsbereich des R^n ist. S bezeichne immer eine Charakteristik von Y, nach Satz 2 ist dann $|S|$ von Null verschieden.

LEMMA 1. *Zu jedem Kompaktum K von Y gibt es ein $\rho(K) = \rho(K; S) > 0$ mit*

$$a'Sy \geqq \rho(K)\,|y|$$

für alle a aus K und alle y aus $\bar{Y}$.

Beweis: Mann kann ohne Einschränkung $y \neq 0$ voraussetzen und wegen der Homogenität beider Seiten der Behauptung genügt es, wenn das Lemma für alle a aus K und y aus $\bar{Y}$ mit $|y| = 1$ bewiesen wird. Da dies eine kompakte Punktmenge in $\bar{Y} \times \bar{Y}$ darstellt, nimmt $a'Sy$ als stetige Funktion ihr Minimum a'_0Sy_0 in einem Punkte (a_0, y_0) an. Nach Satz 1a ist dieses Minimum aber positiv.

Wendet man Lemma 1 auf $K = \{a\}$, a aus Y, an, dann erhält man

$$a'Sy \geqq \rho(a)\,|y| \quad \text{für alle } y \text{ aus } \bar{Y}$$

und wir wollen—um die Bezeichnung eindeutig zu fixieren—stets

$$\rho(a) = \inf\{a'Sy : y \text{ aus } \bar{Y}, |y| = 1\}$$

setzen.

In **2** hatten wir zu jedem Positivitätsbereich eine Halbordnung definiert. Wir können jetzt zeigen, dass im vorliegenden Falle diese Halbordnung archimedisch ist.

LEMMA 2. *Zu jedem $a > 0$ und x aus R^n gibt es $\lambda > 0$ mit $\lambda a > x$.*

Beweis: Es genügt, wenn die Existenz eines λ mit $\lambda a \geqq x$ gezeigt wird, denn dann ist $(\lambda + 1)a > x$. Wäre diese Behauptung aber falsch, d. h. gibt es a aus Y und x aus R^n mit $\lambda a - x \notin \bar{Y}$ für alle $\lambda > 0$, dann gibt es zu jedem λ ein c_λ mit

$$c'_\lambda S(\lambda a - x) < 0, \quad |c_\lambda| = 1, \quad c_\lambda \text{ aus } Y.$$

Jetzt ist mit Lemma 1

$$0 < \rho(a) \leqq c'_\lambda Sa/\lambda < c'_\lambda Sx \leqq |Sx|/\lambda$$

und das ist für $\lambda \to \infty$ ein Widerspruch.

Man kann im Anschluss an Lemma 2 leicht zeigen, dass sich jedes x in der Form $x = a - b$ mit a, b aus Y schreiben lässt. Man hat zu gegebenen $a > 0$ und x nur λ so zu bestimmen, dass $b = \lambda a - x$ in Y liegt. Die nicht ausgearteten Positivitätsbereiche des R^n sind also auch Positivitätsbereiche im Sinne von N. Bourbaki.

Lemma 1 hat aber noch weitere Konsequenzen. Z.B. ist sofort zu sehen, dass die y aus $\bar{Y}$ mit $a \geqq y$ $(a > 0)$ eine beschränkte Punktmenge bilden. Ist weiter y_ν eine Folge aus $\bar{Y}$, für die bei geeigneten $a > 0$ die Folge $a'Sy_\nu$ konvergiert, dann ist y_ν von selbst beschränkt. Für beliebiges a ist dies natürlich keineswegs richtig.

Geometrisch kann man $\rho(a)$ so interpretieren, dass $\rho(a)$ ein Mass für den Abstand des Punktes a von $Rd(Y)$ angibt. Um dies hinreichend allgemein formulieren zu können, sagen wir, dass eine Folge a_ν uneigentlich nach Unendlich konvergiert $(a_\nu \to \infty)$, wenn $|a_\nu|$ über alle Grenzen wächst, und nennen ausserdem a_ν (uneigentlich) gegen einen Randpunkt von Y konvergent $(a_\nu \to Rd(Y))$, wenn $a_\nu \to \infty$ und $|a_\nu|^{-1} a_\nu$ gegen einen Randpunkt konvergiert. Jetzt kann man zeigen, dass eine (eigentlich oder uneigentlich) konvergente Folge a_ν aus Y mit $\rho(a_\nu) \to 0$ stets gegen einen Randpunkt konvergiert. Ist nämlich $a_\nu \to a \neq \infty$ und $\rho(a_\nu) \to 0$ und wäre a kein Randpunkt, dann ist $\rho(a) > 0$. Andererseits gibt es aber eine Folge y_ν aus $\bar{Y}$ mit $\rho(a_\nu) = a'_\nu S y_\nu$, $|y_\nu| = 1$, und man kann $y_\nu \to y$ annehmen. Es folgt $\rho(a_\nu) \to a'Sy \geqq \rho(a)$ und das ist ein Widerspruch. Im Falle $a_\nu \to \infty$ ist $b_\nu = |a_\nu|^{-1} a_\nu$ eigentlich konvergent. Wegen

$$\rho(b_\nu) = |a_\nu|^{-1} \rho(a_\nu) \to 0$$

folgt die Behauptung aber aus dem bereits bewiesenem Teil. Für eigentlich konvergente Folgen kann man diese Aussage umkehren.

5. Automorphismengruppe und Norm eines Positivitätsbereiches. Für nicht ausgeartete Positivitätsbereiche Y bezeichnen wir mit $\Sigma(Y)$ die multiplikative Gruppe der umkehrbaren reellen n-reihigen Matrizen W mit $W\bar{Y} = \bar{Y}$ und nennen $\Sigma(Y)$ die (lineare) *Automorphismengruppe von* Y. Sie ist offenbar unabhängig von der Auswahl der Charakteristik S von Y.

Für W aus $\Sigma(Y)$ und Charakteristik S von Y setzen wir $W^* = S^{-1} W' S$ und erhalten

LEMMA 3. *Mit W gehört auch W^* zu $\Sigma(Y)$.*

Beweis: Wir zeigen zuerst $W^*\bar{Y} \subseteq \bar{Y}$ für alle W aus $\Sigma(Y)$. Wäre das nicht richtig, dann gibt es ein y aus $\bar{Y}$, für das W^*y nicht in $\bar{Y}$ liegt. Nach Satz 1d gibt es dann a aus Y mit $0 > a'SW^*y = (Wa)'Sy$. Da aber Wa in Y liegt, ist das ein Widerspruch zu (P. 1). Ersetzt man in der bereits bewiesenen Behauptung aber W durch W^{-1}, dann folgt schon $W^*\bar{Y} = \bar{Y}$, d. h. W^* liegt in $\Sigma(Y)$.

Eine auf Y definierte Funktion $f(y)$ möge nun eine *Norm von Y* heissen, wenn die folgenden Axiome erfüllt sind:

(N. 1) $f(y)$ ist auf Y stetig,

(N. 2) $f(y) > 0$ für alle y aus Y,

(N. 3) $f(Wy) = \| W \| f(y)$ für alle W aus $\Sigma(Y)$.

Dabei bedeutet $\| W \|$ den absoluten Betrag der Determinante $| W |$ von W. Die Existenz wenigstens einer Norm für jedes Y wird sich später zeigen. Da für $\lambda > 0$ und Einheitsmatrix E die Matrix λE zu $\Sigma(Y)$ gehört, zeigt (N. 3), dass jede Norm eine homogene Funktion von Grade n ist. Ebenfalls wegen (N. 3) ergibt sich trivial, dass

$$dv = dy/f(y), \qquad dy = \prod_{k=1}^{n} dy^k$$

ein bei den Abbildungen $y \to Wy$, W aus $\Sigma(Y)$, invariantes Volumenelement darstellt. Es ist leicht zu sehen, dass umgekehrt Y sicher dann eine Norm besitzt, wenn es ein in diesem Sinne invariantes Volumenelement besitzt.

Wir wollen nun zeigen, dass jedes Y wenigstens eine Norm zulässt und definieren dazu für y aus Y

$$N(y) = \omega/M(y), \qquad M(y) = \int_Y e^{-y'St}\, dt$$

mit einer positiven Konstanten ω, die wir erst später festlegen wollen. Da es zu jedem Kompaktum K von Y nach Lemma 1 ein $\rho(K) > 0$ mit $y'St \geqq \rho(K) | t |$ für alle y aus K und t aus $\bar{Y}$ gibt, ist die Konvergenz des Integrals $M(y)$ sichergestellt und $N(y)$ ist in Y sogar *reell-analytisch.* (N. 1) und (N. 2) für $N(y)$ sind dann trivial. Ist nun W aus $\Sigma(Y)$ gegeben, dann substituiert man in $M(Wy)$

$$t = W^{*-1}x, \qquad dt = \| W \|^{-1}\, dx.$$

Wegen Lemma 3 erhält man als Integrationsgebiet wieder Y und hat daher auch (N. 3) nachgewiesen.

Die Norm $N(y)$ ist also reell-analytisch und ausserdem noch monoton, denn wir hatten schon gesehen, dass aus $a > b > 0$ immer $a'St > b'St$ folgt und das liefert $N(a) > N(b)$.

*Z*um Schluss wollen wir noch einige Eigenschaften von $\Sigma(Y)$ zusammenstellen. Es wird sich dabei zeigen, dass diejenige Untergruppen von $\Sigma(Y)$, deren Elemente W der Bedingung $\| W \| = 1$ genügen, abgeschlossen ist.

Lemma 4. *Es sei W_ν eine Folge von Matrizen aus $\Sigma(Y)$.*

a) *Ist $W_\nu \to W$ konvergent, dann liegt W für $|W| \neq 0$ in $\Sigma(Y)$, im Falle $|W| = 0$ gilt $W\bar{Y} \subseteq Rd(Y)$ und es ist $W = 0$ falls $Wa = 0$ für ein a aus Y.*

b) *Ist $W_\nu a$ für ein a aus Y beschränkt, dann ist auch W_ν beschränkt.*

Beweis: a) Man hat nach Definition $W_\nu \bar{Y} = \bar{Y}$ und $W_\nu^{-1} \bar{Y} = \bar{Y}$. Da aber wegen $|W| \neq 0$ auch die Folge W_ν^{-1} konvergiert, folgt $W\bar{Y} \subseteq \bar{Y}$ und $W^{-1}\bar{Y} \subseteq \bar{Y}$.

Im Falle $|W| = 0$ gilt sicher $W\bar{Y} \subseteq \bar{Y}$. Wäre jetzt $W\bar{Y}$ keine Teilmenge von $Rd(Y)$, dann gibt es a aus Y mit $Wa \in Y$. Wegen (N. 1, 3) folgt dann

$$0 < N(Wa) = \lim_{\nu \to \infty} N(W_\nu a) = \lim_{\nu \to \infty} \| W_\nu \| N(a) = 0,$$

also ein Widerspruch.

Für die letzte Aussage von a) zeigen wir zuerst, dass auch $W^* a = 0$. Wäre nämlich $W^* a \neq 0$, dann ist nach Satz 1a

$$0 < a'SW^*a = (Wa)'Sa = 0.$$

Ist nun y beliebig aus Y gewählt, dann liegt Wy in $\bar{Y}$. Wäre $Wy \neq 0$, dann wieder nach Satz 1a

$$0 < a'SWy = (W^*a)'Sy = 0.$$

Es ist also $Wy = 0$ für alle y aus Y, d. h. $W = 0$.

b) Für alle y aus Y mit $|Sy| \leqq 1$ folgt nach Lemma 1

$$y'SW_\nu a > \rho(a) \,|\, W^*_\nu y \,|.$$

Andererseits sind die Elemente von $W_\nu a$ beschränkt, d. h. $| W_\nu a | \leqq \gamma_1$ und man hat[3]

$$| W^*_\nu y | \leqq | Sy | \, | W_\nu a | / \rho(a) \leqq \gamma_2$$

---

[3] γ_1, γ_2 usw. bezeichnen positive von ν unabhängige Zahlen.

oder $y'W^{*\prime}_\nu W^*_\nu y \leqq \gamma_3$. Jetzt ergibt sich aber leicht, dass dann die Elemente von W^*_ν und daher auch von W_ν beschränkt sind.

In ähnlicher Weise kann man noch zeigen, dass für jedes a aus Y die Gruppe der W aus $\Sigma(Y)$ mit $Wa = a$ kompakt ist.

6. Ein invariantes Linienelement von Y. Es sei von nun an stets $N(y)$ die spezielle reell-analytische Norm von Y nach **5.** Ein positiv definites Linienelement

$$ds^2 = \sum_{k,l} g_{kl}(y)\,dy^k dy^l$$

möge *bei* $\Sigma(Y)$ *invariant* heissen, wenn die durch ds definierte Massbestimmung von Y bei den Bewegungen $y \to Wy$, W aus $\Sigma(Y)$, invariant ist. Bekanntlich ist dies dann und nur dann der Fall, wenn

$$W' \cdot G(Wy) \cdot W = G(y), \qquad G(y) = (g_{kl}(y))$$

für jedes W aus $\Sigma(Y)$ erfüllt ist.

Satz 3. *Das Linienelement*

$$ds^2 = \sum_{k,l} h_{kl}(y)\,dy^k dy^l, \qquad h_{kl}(y) = -\partial^2 \log N(y)/\partial y^k \partial y^l$$

ist positiv definit und bei $\Sigma(Y)$ *invariant.*

Beweis: Die Invarianz dieses Linienelementes folgt trivial aus (N. 3). Es muss lediglich gezeigt werden, dass $H(y) = (h_{kl}(y))$ in jedem Punkt y von Y als Matrix einer quadratischen Form positiv definit ist. Setzt man dazu $z = St$ und

$$M_k = \partial M(y)/\partial y^k = -\int_Y e^{-y'z} z^k\,dt,$$

$$M_{kl} = \partial^2 M(y)/\partial y^k dy^l = \int_Y e^{-y'z} z^k z^l\,dt,$$

dann folgt für x aus R^n

$$\begin{aligned}
2[M(y)]^2 x'H(y)x &= 2\sum_{k,l} x^k x^l (M \cdot M_{kl} - M_k \cdot M_l)\\
&= \sum_{k,l} x^k x^l (M \cdot M_{kl} + M \cdot M_{lk} - 2M_k M_l)\\
&= \sum_{k,l} x^k x^l \int_Y dt_1 \int_Y dt_2\; e^{-y'(z_1+z_2)} (z_1^k z_1^l + z_2^k z_2^l - 2z_1^k z_2^l)\\
&= \int_Y dt_1 \int_Y dt_2 e^{-y'(z_1+z_2)} [(x'z_1)^2 + (x'z_2)^2 - 2(x'z_1)(x'z_2)]\\
&= \int_Y dt_1 \int_Y dt_2\, e^{-y'(z_1+z_2)} [x'S(t_1 - t_2)]^2
\end{aligned}$$

und daher ist $x'H(y)x > 0$ für $x \neq 0$, d. h. $H(y)$ positiv definit.

Aus einem invarianten Linienelement kann man bekanntlich eine *invariante Metrik* konstruieren. Sei dazu C eine ganz in Y liegende Kurve mit der Parameterdarstellung $y=y(\tau)$, $\alpha \leqq \tau \leqq \beta$, bei der die Komponenten von $y(\tau)$ stückweise stetig differenzierbare Funktionen der (reellen) Variablen τ sind. Wie üblich definiert man dann die *Länge von* C in der durch das Linienelement nach Satz 3 gegebenen Massbestimmung durch

$$\lambda(C)=\left|\int_\alpha^\beta (\dot{y}'H(y)\dot{y})^{\frac{1}{2}}d\tau\right|.$$

Da ds bei $\Sigma(Y)$ invariant ist, folgt sofort $\lambda(WC)=\lambda(C)$ für jedes W aus $\Sigma(Y)$. Setzt man ausserdem für a und b aus Y

$$\lambda(a,b)=\inf\{\lambda(C): y(\alpha)=a, y(\beta)=b, C\subset Y\}.$$

dann überlegt man sich sofort, dass $\lambda(a,b)$ eine bei $\Sigma(Y)$ invariante Metrik von Y darstellt, d. h. den folgenden Forderungen genügt:

(M. 1) $\lambda(a,b)=\lambda(b,a)\geqq 0$, $\lambda(a,b)=0$ nur bei $a=b$,

(M. 2) $\lambda(a,b)\leqq\lambda(a,c)+\lambda(c,b)$ für a, b und c aus Y,

(M. 3) Es gibt zu jedem Kompaktum K von Y zwei Konstanten $\gamma>0$ und $\gamma'>0$ mit $\gamma\,|a-b|\leqq\lambda(a,b)\leqq\gamma'\,|a-b|$ für alle a und b aus K, d. h. die durch $\lambda(a,b)$ in Y induzierte Topologie ist mit der natürlichen Topologie des R^n äquivalent,

(M. 4) Für jedes W aus $\Sigma(Y)$ ist $\lambda(Wa,Wb)=\lambda(a,b)$.

Zwei Probleme drängen sich in diesem Zusammenhang auf:

(A) Ist es richtig, dass für Positivitätsbereiche die geodätischen Linien der hier angegebenen Massbestimmung eindeutig bestimmt sind?

(B) Ist die Metrik $\lambda(a,b)$ *vollständig*, d. h. strebt für jede Folge a_ν auf Y, die gegen einen Randpunkt von Y konvergiert, der Abstand $\lambda(a,a_\nu)$, a aus Y, gegen Unendlich?

Eine Klärung dieser beiden Fragen wäre von grossem Interesse.

7. Positivitätsbereiche mit Involution. Wie bisher sei S eine Charakteristik von Y und $W^*=S^{-1}W'S$. Wir hatten schon gesehen, dass mit W auch W^* in $\Sigma(Y)$ liegt.

Eine Abbildung $y\rightarrow y^*$ von Y auf sich soll eine *Involution von* Y genannt werden, wenn für alle y aus Y gilt:

(I. 1) $(y^*)^* = y$,

(I. 2) $N(y)N(y^*) = \text{const.}$,

(I. 3) $(Wy)^* = W^{*-1}y^*$ für alle W aus $\Sigma(Y)$.

In diesem Abschnitt wollen wir zeigen, dass jeder nicht ausgearteter Positivitätsbereich wenigstens eine Involution zulässt.

Für eine auf Y definierte und dort einmal partiell differenzierbare Funktion $f(y)$ setzt man wie üblich

$$\operatorname{grad}_y f(y) = \begin{bmatrix} \partial f(y)/\partial y^1 \\ \cdot \\ \cdot \\ \cdot \\ \partial f(y)/\partial y^n \end{bmatrix}.$$

Zu jedem y aus Y definieren wir jetzt ein y^* durch

$$y^* = S^{-1} \operatorname{grad}_y \log N(y).$$

Man sieht sofort, dass sich die Euler'sche Differentialgleichung für die homogene Funktion $N(y)$ in der Form $y'Sy^* = n$ schreiben lassen. Sei weiter für alle y aus Y

$$H(y) = -(\partial^2 \log N(y)/\partial y^k \partial y^l), \qquad K(y) = -(\partial y^{*k}/\partial y^l).$$

dann erkennt man sofort die Richtigkeit von $H(y) = SK(y)$ und daher ist stets $|K(y)| \neq 0$, denn $H(y)$ war nach Satz 3 positiv definit. Man kann also auch y als Funktion der Komponenten von y^* auffassen und erhält dann leicht $K(y)K(y^*) = E$. Man beachte hier aber, dass bis jetzt keineswegs bewiesen ist, dass y^* auch zu Y gehört. Durch Differentiation von $y'Sy^* = n$ erhält man schliesslich noch $y^* = K(y)y$ für alle y aus Y.

SATZ 4. *Die Abbildung $y \rightarrow y^*$ ist eine Involution von Y. Man kann $N(y)$ so normieren, dass es ein c aus Y mit $N(c)N(c^*) = 1$ gibt.*

Nach dieser Normierung hat man an Stelle von (I. 2) $N(y)N(y^*) = 1$ für alle y aus Y.

Beweis: Wir teilen den Beweis in mehrere Schritte auf:

1) *Beweis von* (I. 3): Sei W aus $\Sigma(Y)$, $Wy = z$, dann folgt nach Definition

$$\begin{aligned}(Wy)^* &= S^{-1} \operatorname{grad}_z \log N(z) = S^{-1} \operatorname{grad}_z \log N(y) \\ &= S^{-1}W'^{-1} \operatorname{grad}_y \log N(y) = S^{-1}W'^{-1}Sy^*\end{aligned}$$

und das ist die Behauptung.

2) *Zu jedem a aus Y gibt es ein b aus Y mit $a = b^*$.* Man fragt dazu für gegebenes a aus Y nach dem Minimum der Linearform $a'Sy$ unter den Nebenbedingungen $N(y) = \eta$ $(\eta > 0)$ und y aus $\bar{Y}$. Dieses Minimum wird in einem Punkt b von $\bar{Y}$ angenommen und nach der Methode von Lagrange erhält man als Bestimmungsgleichungen für b

$$a = \lambda b^*, \qquad N(b) = \eta.$$

Nach der ersten Gleichung liegt also entweder b^* oder $-b^*$ in Y. Wegen $b'Sb^* = n$ kann aber nur b^* ein Punkt von Y sein. Wegen 1) kann man jetzt aber $a = (1/\lambda\, b)^*$ schreiben und das ist die Behauptung

3) *Für alle a und y aus Y ist $a'Sy^* \geqq 0$.* $N(y)$ war nach **5** reell-analytisch, d.h. $\log N(y + \lambda a)$ ist in eine gewöhnliche Potenzreiche nach Potenzen von λ entwickelbar:

$$\log N(y + \lambda a) = \log N(y) + \lambda a'Sy^* + \cdots,$$

d.h. $\log\{N(y + \lambda a)/N(y)\} = \lambda a'Sy^* + \cdots$. Nach **5** war $N(y)$ ausserdem monoton, d.h. für $\lambda > 0$ gilt $N(y + \lambda a) > N(y)$. Für $\lambda \to 0$ folgt dann aber schon die behauptete Ungleichung.

4) *$y \to y^*$ ist Abbildung von Y auf sich.* Nach 2) erhält man als Bild von Y bei dieser Abbildung eine Punktmenge, die Y umfasst. Da diese Abbildung stetig ist, genügt es offenbar, wenn wir noch zeigen, dass die Bildmenge in $\bar{Y}$ enthalten ist. Würde jetzt aber für ein y aus Y das zugehörige y^* nicht in $\bar{Y}$ liegen, dann gibt es nach Satz 1d ein a aus Y mit $a'Sy^* < 0$. Nach 3) ist dies aber ein Widerspruch.

5) *Beweis von* (I.1,2): Nach den bereits bewiesenen Rechenregeln hat man

$$(y^*)^* = K(y^*)y^* = K(y^*)K(y)y = y.$$

Zum Beweis von (I.2) setzen wir $f(y) = N(y)N(y^*)$ und erhalten

$$\begin{aligned} \operatorname{grad}_y \log f(y) &= \operatorname{grad}_y \log N(y) - K'(y) \operatorname{grad}_{y^*} \log N(y^*) \\ &= Sy^* - K'(y)S(y^*)^* = SK(y)(y - y^{**}) = 0, \end{aligned}$$

denn $SK(y)$ war symmetrisch.

6) *Normierung von $N(y)$*: Man gibt sich ein a aus Y vor und setzt in der Bezeichnung von **5**

$$M(a) = \alpha^n, \qquad M(a^*) = \beta^n, \quad \alpha > 0, \quad \beta > 0.$$

Bei $c=\sqrt{\alpha/\beta}\,a$ folgt $M(c)=M(c^*)$. Die Konstate ω in der Definition von $N(y)$ fixieren wir jetzt durch $\omega=M(c)=M(c^*)$ und erhalten die noch fehlende Behauptung.

Die hier definierten Matrizen $K(y)$ sind über die bisherigen Zusammenhange hinaus deswegen von besonderem Interesse, weil in allen bekannten Beispielen die folgende Frage positiv beantwortet werden kann:

(C) Gehört für jedes y aus Y die Matrix $K(y)$ zu $\Sigma(Y)$?

Eine allgemeine Lösung dieses Problems würde für Positivitätsbereiche einen Einblick in die Automorphismengruppe ermöglichen. In Richtung auf (C) kann man jedoch vorläufig nur beweisen, dass die folgenden drei Aussagen gleichbedeutend sind:

(1) Für jedes y aus Y gehört $K(y)$ zu $\Sigma(Y)$.

(2) Für alle a und y aus Y und hinreichend kleines $\lambda>0$ gilt

$$y^*\geqq(y+\lambda a)^*.$$

(3) Für alle a und b aus Y mit $a>b$ gilt stets $b^*>a^*$.

Der Beweis dieser Äquivalenz soll übergangen werden.

Ausser den bisher erwähnten Eigenschaften der Involution $y\rightarrow y^*$ ist noch bemerkenswert, dass diese Involution mit der Metrik $\lambda(a,b)$ verträglich ist, d.h. es gilt $\lambda(a^*,b^*)=\lambda(a,b)$ für je zwei Punkte a und b von Y. Diese Invarianz ist leicht nachzuweisen, wenn man beachtet, dass für eine Parameterdarstellung $y(\tau)$ einer Kurve C von Y das Bild C^* von C bei der Abbildung $y\rightarrow y^*$ die Parameterdarstellung $y^*(\tau)$ hat. Ohne Schwierigkeiten zeigt man damit $\lambda(C)=\lambda(C^*)$ und der Übergang zum Infimum liefert die obige Behauptung.

8. Homogene Positivitätsbereiche. Einen nicht ausgearteten Positivitätsbereich Y nennen wir *homogen*, wenn es zu je zwei Punkten a und b aus Y ein W aus $\Sigma(Y)$ mit $a=Wb$ gibt. Es soll von jetzt immer vorausgesetzt werden, dass Y ein homogener Positivitätsbereich ist. Wegen (N. 3) in **5** ist eine Norm von Y dann bis auf einen konstanten Faktor eindeutig bestimmt.

Das Verhalten von $N(y)$ auf dem Rand von Y kann man vollständig übersehen, denn es gilt:

LEMMA 5. *Ist $a_\nu\rightarrow a$, a aus $Rd(Y)$, eine (eigentlich) konvergente Folge aus Y, dann konvergiert $N(a_\nu)$ gegen Null.*

Beweis: Wir wählen einen Punkt c von Y und bestimmen W_ν aus $\Sigma(Y)$ mit $a_\nu = W_\nu c$. Da die a_ν beschränkt sind, sind nach Lemma 4b die Matrizen W_ν beschränkt und wir können ohne Einschränkung annehmen, dass W_ν gegen eine Matrix W konvergiert. Wäre hier $|W| \neq 0$, dann liegt W nach Lemma 4a in $\Sigma(Y)$ und a könnte kein Randpunkt sein. Es ist also $|W| = 0$ und wegen $N(a_\nu) = \| W_\nu \| N(c)$ folgt die Behauptung.

Nach diesem Lemma ist also $N(y)$ stetig auf $\bar{Y}$ fortsetzbar und wir bezeichnen diese Fortsetzung wieder mit $N(y)$.

Man könnte in Analogie zu diesem Lemma vermuten, dass für jede gegen Unendlich konvergierende Folge auch die Norm nach Unendlich konvergiert. Dies ist jedoch nicht allgemein richtig, es gilt vielmehr nur

LEMMA 6. *Für jede Folge $a_\nu \geqq a > 0$, die gegen Unendlich konvergiert, strebt auch $N(a_\nu)$ gegen Unendlich.*

Beweis: Mit geeigneten W_ν aus $\Sigma(Y)$ kann man $a_\nu = W_\nu a$ schreiben, d.h. es ist $a \geqq W_\nu^{-1} a$, und die Vektoren $W_\nu^{-1} a$ sind beschränkt. Wegen Lemma 4b sind dann wieder die Matrizen W_ν^{-1} beschränkt und man kann ohne Einschränkung $W_\nu^{-1} \rightarrow W$ annehmen. Wäre hier aber $|W| \neq 0$, dann würde auch die Folge W_ν konvergieren. Da dies der Voraussetzung widerspricht, ist $|W| = 0$ und das ist die Behauptung.

Wir kommen nun zu zwei wichtigen Eindeutigkeitssätzen. Es zeigt sich nämlich, dass ein Positivitätsbereich, wenn er homogen ist, durch seine Norm eindeutig bestimmt ist.

SATZ 5. *Sind Y_1 und Y_2 zwei homogene Positivitätsbereiche mit den Normen $N_1(y)$ und $N_2(y)$ und gilt*

$$Y_1 \cap Y_2 \neq \emptyset, \quad N_1(y) = N_2(y) \text{ für alle } y \text{ aus } Y_1 \cap Y_2,$$

dann ist $Y_1 = Y_2$.

Beweis: Es genügt, wenn wir

$$Rd(Y_1) \cap Y_2 = Rd(Y_2) \cap Y_1 = \emptyset$$

nachweisen, denn da Y_1 und Y_2 offene konvexe Mengen sind, folgt hieraus der Satz. Zum Beweis dieser Behauptung setzen wir für y aus $Y_1 \cup Y_2$

$$N(y) = N_1(y), \text{ falls } y \text{ aus } Y_1, \quad N(y) = N_2(y), \text{ falls } y \text{ aus } Y_2.$$

Nach Voraussetzung ist diese Definition eindeutig. Würde es nun einen Punkt a aus $Rd(Y_1) \cap Y_2$ geben, dann wählt man eine Folge a_ν aus $Y_1 \cap Y_2$, die gegen a konvergiert. Jetzt folgt aber

$$0 < N_2(a) = \lim_{\nu \to \infty} N_2(a_\nu) = \lim_{\nu \to \infty} N_1(a_\nu) = 0$$

unter Verwendung von Lemma 5. Dieser Widerspruch löst sich nur, wenn die obige Behauptung richtig ist.

Nach diesem Eindeutigkeitssatz ist es jetzt möglich, die Automorphismengruppe $\Sigma(Y)$ auf eine neue Art zu charakterisieren. Es zeigt sich nämlich, dass $\Sigma(Y)$ genau aus den "Einheiten" der Funktion $N(y)$ besteht.

SATZ 6. *Eine reelle nicht ausgeartete Matrix W gehört dann und nur dann zu $\Sigma(Y)$, wenn $WY \cap Y \neq \emptyset$ und $\| W \| \cdot N(W^{-1}y) = N(y)$ für alle y aus $WY \cap Y$.*

Beweis: Dass die W aus $\Sigma(Y)$ den angeführten Bedingugen genügen, ist sicher richtig. Sei also umgekehrt W eine reelle umkehrbare Matrix mit den angegebenen Eigenschaften. Wegen der Homogenität von $N(y)$ können wir ohne Einschänkung $\| W \| = 1$ annehmen. Bei $\tilde{Y} = WY$ hat man nach Voraussetzung

$$Y \cap \tilde{Y} \neq 0, \qquad N(W^{-1}y) = N(y) \text{ für alle } y \text{ aus } Y \cap \tilde{Y}.$$

$\tilde{Y}$ ist wieder homogener Positivitätsbereich und wir können als Norm $\tilde{N}(y) = N(W^{-1}y)$, y aus $\tilde{Y}$, nehmen. Nach Voraussetzung ist dann aber $N(y) = \tilde{N}(y)$ für alle y aus $Y \cap \tilde{Y}$ und Satz 5 ergibt $Y = \tilde{Y}$, d.h. W ist ein Element von $\Sigma(Y)$.

In **5** hatte man gesehen, dass das Volumenelement $dv = (dy)/N(y)$ bei den Abbildungen $y \rightarrow Wy$, W aus $\Sigma(Y)$, invariant ist. Da man andererseits ein Volumenelement der durch $H(y)$ (vergl. **6**) definierten Massbestimmung in der Form $\sqrt{|H(y)|}\,dy$ erhält und dies für homogene Positivitätsbereiche bis auf einen konstanten Faktor eindeutig bestimmt ist, folgt $N^2(y) \cdot |H(y)| = \alpha$. Nach den Überlegungen von **7** hat man jetzt

$$dv^* = \frac{1}{N(y^*)}\, dy^* = \| K(y) \| \, N(y) dy = \frac{\alpha}{\| S \| \; N(y)}\, dy = \frac{\alpha}{\| S \|}\, dv$$

Erstetzt man in dieser Gleichung y durch y^*, so folgt $\alpha = \| S \|$ und man hat

$$dv^* = dv, \qquad |H(y)| = \| S \| / N^2(y)$$

nachgewiesen.

9. Die Fläche $N(y) = 1$. Ist Y wieder ein homogener Positivitätsbereich, dann wollen wir unter der *Normfläche von Y* die Menge der y aus Y mit $N(y) = 1$ verstehen. Wegen der Homogenität von $N(y)$ ist diese Normfläche zusammenhängend.

Wir werden zeigen, dass sich die Normfläche für $y \rightarrow \infty$ überall an den

Rand von Y anschmiegt. Nach den Überlegung von **4** genügt es, wenn man $\rho(y)\to 0$ für $y\to\infty$ unter der Nebenbedingung $N(y)=1$ nachweist.

Man überlegt sich dazu zuerst, dass für $N(y_\nu)=1$ die beiden Aussagen $y_\nu\to\infty$ und $y^*{}_\nu\to\infty$ gleichbedeutend sind. Ist nämlich zum Beispiel $y_\nu\to\infty$ und würde es eine beschränkte konvergente Teilfolge der $y^*{}_\nu$ geben, dann können wir ohne Einschränkung $y^*{}_\nu\to a$ annehmen und a ist dann sicher ein Randpunkt von Y. Nach Lemma 5 strebt $N(y^*{}_\nu)$ gegen Null und $N(y_\nu)N(y^*{}_\nu)=1$ ergibt einen Widerspruch.

Wendet man Lemma 1 auf die in **7** bewiesene Gleichung $y'Sy^*=n$ an, so folgt $\rho(y)\,|\,y^*\,|\leqq n$ für alle y aus Y, d.h. $\rho(y)\to 0$ falls $y^*\to\infty$. Wir hatten ober oben schon gesehen, dass für $y\to\infty$, $N(y)=1$, auch $y^*\to\infty$ gilt, so dass also

$$\rho(y)\to 0 \text{ falls } y\to\infty, N(y)=1$$

richtig ist.

10. Die Gamma-Funktion eines Positivitätsbereiches. Wie bisher sei Y ein homogener Positivitätsbereich. In Verallgemeinerung der Euler'schen Definition der Γ-Funktion definieren wir für eine komplexe Variable s mit $\operatorname{Re}s\geqq 1$ und a aus Y die *Gamma-Funktion* von Y durch

$$\Gamma(Y,s)=[N(a)]^s\int_Y e^{-a'Sy}[N(y)]^{s-1}\,dy.$$

Zum Nachweis der Konvergenz dieses Integrals überlegt man sich, dass $N(y)\leqq\rho\,|\,y\,|^n$ mit geeignetem $\rho>0$ für alle y aus Y gilt. Lemma 1 zeigt dann, dass $\Gamma(Y,s)$ für $\operatorname{Re}s\geqq 1$ absolut konvergiert und dort eine holomorphe Funktion von s darstellt. Wegen der Homogenität von Y ist sofort zu sehen, dass die rechte Seite nicht von der Wahl des Punktes a abhängt.

Eine genauere Untersuchung dieser Gamma-Funktion wäre von Interesse, denn man kann $\Gamma(Y,s)$ als einfachste analytische Invariante von Y auffassen. Es ist zu vermuten, dass $\Gamma(Y,s)$ sich bis auf elementare Faktoren als Produkt von Funktionen der Form $\Gamma(\alpha s+\beta)$ schreiben lässt. Für eine einfache Klasse von Bereichen wurde dies von S. Bochner bewiesen.

Wir wollen jetzt eine wichtige Klasse von Integralen über Y berechnen, d.h. auf $\Gamma(Y,s)$ zurückführen.

LEMMA 7. *Ist $f(x)$ für positive x stückweise stetig und existiert für* $\operatorname{Re}s\geqq 1$ *das Integral*

$$I(f;s)=\int_0^\infty f(x)x^{ns-1}\,dx$$

absolut, dann gilt für diese s

$$\int_Y f(a'Sy)[N(y)]^{s-1}dy=\frac{I(f;s)\Gamma(Y,s)}{\Gamma(ns)[N(a)]^s}.$$

Beweis: Es sei $d\omega(x)$ das durch dy auf der Hyperfläche $|y|=x$ induzierte Flächenelement, d. h. $d\omega(x)=x^{n-1}d\omega$, wobei dann $d\omega$ das Flächenelement für $|y|=1$ ist. Jetzt hat man für das zu bestimmende Integral

$$\int_0^\infty dx\int_{|y|=1} d\omega\, x^{n-1}f(x\cdot a'Sy)[N(xy)]^{s-1}$$
$$=\int_0^\infty f(x)x^{ns-1}\,dx\int_{|y|=1}[N(y)]^{s-1}(a'Sy)^{-ns}\,d\omega=I(f;s)\cdot I(a),$$

wobei also das zweite Integral mit $I(a)$ bezeichnet ist. Zur Bestimmung $I(a)$ setzt man $f(x)=e^{-x}$ und erhält

$$[N(a)]^{-s}\Gamma(Y,s)=\Gamma(ns)\cdot I(a)$$

also die Behauptung.

Eine weitere Integralbeziehung geben wir ohne Beweis an: Es gilt für $\operatorname{Re} s\geqq 1$

$$\int_Y\frac{dy}{[N(a+y)]^{s+1}}=\frac{\omega}{[N(a)]^s}\,\frac{\Gamma(Y,s)}{\Gamma(Y,s+1)}$$

und das linke Integral konvergiert absolut. Dabei bedeutet ω die zur Normierung von $N(y)$ in **5** benutzte Konstante.

11. Beispiele von Positivitätsbereichen.

a) *Der triviale Bereich.* Es sei Y^n die Menge der Vektoren des R^n mit positiven Komponenten und S eine beliebige symmetrische Permutationsmatrix von n Zeilen, d. h. eine symmetrische Matrix, bei der in jeder Zeile und jeder Spalte genau eine 1 und sonst Nullen stehen. Offenbar ist Y^n ein nicht ausgearteter Positivitätsbereich mit S als Charakteristik, den wir auch den *trivialen Bereich* des R^n nennen wollen. Schon an diesem einfachen Beispiel sieht man, dass die Charakteristik S keineswegs immer positiv definit ist, unter den symmetrischen Permutationsmatrizen kommen vielmehr alle möglichen Signaturen vor.

Nach **5** berechnet man die Norm bis auf einen konstanten Faktor zu

$$N(y)=\prod_k y^k \text{ und } ds^2=\sum_k (dy^k/y\ )^2.$$

Für die Involution nach **7** findet man $y^{*'}=S^{-1}(1/y^1,1/y^2,\cdots,1/y^n)$. Ohne Schwierigkeiten zeigt man ferner, dass die Automorphismengruppe $\Sigma(Y^n)$

genau aus den Produkten PD einer Permutationsmatrix P und einer Diagonalmatrix D mit positiven Diagonalelementen besteht. Die Gamma-Funktion von Y^n erhält man in der Form $\Gamma(Y^n, s) = [\Gamma(s)]^n$.

b) *Positive quadratische Formen.* Sei m eine natürliche Zahl und $n = m(m+1)/2$. Für jede symmmetrische m-reihige reelle Matrix $\mathfrak{Y} = (y_{kl})$ setzen wir

$$f(\mathfrak{Y}) = (y_{11}, y_{22}, \cdots, y_{mm}, y_{12}, y_{13}, \cdots, y_{m-1,m})'.$$

Die Abbildung $\mathfrak{Y} \to f(\mathfrak{Y})$ ist dann eine eineindeutige Abbildung des Raumes aller symmetrischen reellen Matrizen von m Zeilen auf den R^n. Sei nun

$$Y_P^{(m)} = \{y : y = f(\mathfrak{Y}), \mathfrak{Y}^{(m)} \text{ positiv definit}\}$$

$$S = \begin{bmatrix} 1 & & & & & \\ & \ddots & & & 0 & \\ & & 1 & & & \\ & & & 2 & & \\ & 0 & & & \ddots & \\ & & & & & 2 \end{bmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}1\\ \ddots\\ 1\end{matrix}}\right\} m \\ \left.\vphantom{\begin{matrix}2\\ \ddots\\ 2\end{matrix}}\right\} n-m \end{matrix}$$

dann prüft man leicht, dass für $a = f(\mathfrak{A})$ und $y = f(\mathfrak{Y})$ stets

$$a'Sy = Spur(\mathfrak{A}\mathfrak{Y})$$

erfüllt ist. Offenbar ist dann $Y_P^{(m)}$ ein nicht ausgearteter Positivitätsbereich des R^n.

Ist $\mathfrak{R}$ eine reelle nicht ausgeartete Matrix von m Zeilen, so liefert $\mathfrak{Y} \to \mathfrak{R}'\mathfrak{Y}\mathfrak{R}$ eine eineindeutige Abbildung der positiv definiten Matrizen auf sich und in

$$f(\mathfrak{R}'\mathfrak{Y}\mathfrak{R}) = Wf(\mathfrak{Y}), \qquad W = W^{(n)} = W(\mathfrak{R})$$

hängt die Matrix W nur von $\mathfrak{R}$ ab und ihre Komponenten sind homogene quadratische Polynome in den Elementen von $\mathfrak{R}$. Die Gruppe Σ_0 der Matrizen $W = W(\mathfrak{R})$, $|\mathfrak{R}| \neq 0$, ist eine Untergruppe von $\Sigma(Y_P^{(m)})$, es ist leicht zu zeigen, dass Σ_0 mit der Automorphismengruppe übereinstimmt. Man sieht aber sofort, dass schon Σ_0 auf $Y_P^{(m)}$ transitiv wirkt, d. h. der Positivitätsbereich homogen ist. Ohne Schwierigkeiten findet man

$$\begin{aligned} N(y) &= |\mathfrak{Y}|^{(m+1)/2}, && \text{falls } y = f(\mathfrak{Y}), \\ ds^2 &= (m+1)/2\, Spur(\mathfrak{Y}^{-1}\delta\mathfrak{Y}\mathfrak{Y}^{-1}\delta\mathfrak{Y}), && \delta\mathfrak{Y} = (dy_{kl}), \\ y^* &= (m+1)/2\, f(\mathfrak{Y}^{-1}), && \text{falls } y = f(\mathfrak{Y}) \end{aligned}$$

und nach C. L. Siegel ist

$$\Gamma(Y_P{}^{(m)}, s) = \pi^{m(m-1)/4} \prod_{k=0}^{m-1} \Gamma(\tfrac{1}{2}(s[m+1] - k)).$$

c) *Positive hermitesche Formen.* Man setzt hier $n = m^2$ und betrachtet die hemiteschen Matrizen von m Zeilen und Spalten

$$\mathfrak{Z} = \mathfrak{Z}' = (z_{kl}) = \mathfrak{Y} + i\mathfrak{X}, \quad \mathfrak{Y}' = \mathfrak{Y}, \quad \mathfrak{X}' = -\mathfrak{X}.$$

Für schiefsymmetrische Matrizen $\mathfrak{X} = (x_{kl})$ setzen wir analag zu b)

$$g(\mathfrak{X}) = (x_{12}, x_{13}, \cdots, x_{m-1,m})'$$

und definieren in der dortigen Bezeichnung

$$h(\mathfrak{Z}) = \begin{pmatrix} f(\mathfrak{Y}) \\ g(\mathfrak{X}) \end{pmatrix}, \qquad \mathfrak{Z} = \mathfrak{Y} + i\mathfrak{X}.$$

Wie in b) findet man

$$a'Sz = Spur(\mathfrak{A}\mathfrak{Z}), \quad a = h(\mathfrak{A}), \quad z = h(\mathfrak{Z})$$

und weisst nach, dass die Menge $y = h(\mathfrak{Z})$, für die $\mathfrak{Z}$ eine hermitesch positiv definite Matrix ist, einen nicht ausgearteten Positivitätsbereich $Y_P{}^{(m)}$ bilden. Eine hermitesche Matrix $\mathfrak{Z}$ heisst dabei *hermitesch positiv definit,* wenn $\mathfrak{x}'\mathfrak{Z}\mathfrak{x}$ für alle komplexen Vektoren $\mathfrak{x} \neq 0$ positiv ausfällt. Die Norm berechnet man hier zu

$$N(y) = \| \mathfrak{Z} \|^m \text{ falls } y = h(\mathfrak{Z})$$

und nach H. Braun gilt

$$\Gamma(Y_H{}^{(m)}, s) = (2\pi)^{m(m-1)/2} \prod_{k=0}^{m-1} \Gamma(ms + k)$$

d) *Positivitätsbereiche im R^3.* Von einem ganz anderen Typus als die bisherigen Beispiele sind die Bereiche, die wir jetzt untersuchen wollen. Sei dazu

$$0 < \rho < 1, \qquad \alpha = 1/\rho(\rho/(1-\rho))^{1-\rho}, \qquad S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \alpha \end{pmatrix}.$$

Das Ziel dieses letzten Abschnittes ist es, zu zeigen, dass der Bereich

$$Y(\rho) = \{y : y = \begin{pmatrix} u \\ v \\ w \end{pmatrix}, u > 0, v > 0, | w | < u^\rho v^{1-\rho}\}$$

ein Positivitätsbereich des R^3 mit S als Charakteristik ist.

Die Komponenten der Punkte des R^3 bezeichnen wir stets mit u, v und w. Sind jetzt y_1 und y_2 zwei Punkte aus $Y(\rho)$, dann hat man

$$\begin{aligned} y'_1 S y_2 &= u_1u_2 + v_1v_2 + \alpha w_1w_2, \qquad |w_j| < u_j^{\rho} v_j^{1-\rho} \\ &> u_1u_2 + v_1v_2 - \alpha(u_1u_2)^{\rho}(v_1v_2)^{1-\rho} = u_1u_2 p(v_1v_2/u_1u_2) \end{aligned}$$

mit $p(t) = 1 + t - \alpha t^{1-\rho}$. Man überlegt sich sofort, dass $\tau = (1-\rho)/\rho$ das einzige Minimum von $p(t)$ ist. Wegen $p(\tau) = 0$ ist dann aber $p(t) \geqq 0$ für alle $t \geqq 0$. Damit ist (P. 1) nachgewiesen. Ist y_1 dagegen ein Punkt des Komplementes von $Y(\rho)$, dann ist (P. 2) in den Fällen $u_1 \leqq 0$ oder $v_1 \leqq 0$ leicht zu sehen. Sind dagegen u_1 und v_1 beide positiv, dann ist $|w_1| \geqq u_1^{\rho} v_1^{1-\rho}$. Wir wählen jetzt y_2 aus $\bar{Y}(\rho)$ mit den Nebenbedingungen

$$v_1v_2/u_1u_2 = \tau, \quad w_2 = -(w_1/|w_1|)u_2^{\rho} v_2^{1-\rho}$$

und erhalten

$$\begin{aligned} y'_1 S y_2 &= u_1u_2 + v_1v_2 + \alpha w_1w_2 \\ &= u_1u_2 p(\tau) - \alpha(|w_1| - u_1^{\rho} v_1^{1-\rho}) u_2^{\rho} v_2^{1-\rho} \leqq 0, \end{aligned}$$

also ebenfalls (P. 2).

Die Bereiche $Y(\rho)$ sind für $2\rho \neq 1$ bisher nicht untersucht, der Fall $2\rho = 1$ führt auf die positiven quadratischen Formen in zwei Variablen. Da aber alle $Y(\rho)$ gemeinsam mit den in a), b) und c) aufgeführten wichtigen Beispielen als Positivitätsbereiche unter einem gemeinsamen Gesichtspunkt erscheinen, wäre eine Untersuchung der $Y(\rho)$ von grossem Interesse. Es ist zu vermuten, dass die $Y(\rho)$, $2\rho \neq 1$, nicht mehr homogen sind.

Man kann schliesslich noch ohne grosse Schwierigkeiten zeigen, dass die Bereiche

$$Y^3, \; Y_P^{(2)} \text{ und } Y(\rho) \qquad (0 < \rho < \tfrac{1}{2})$$

bis auf affine Abbildungen *alle* Positivitätsbereiche des R^3 liefern. Eine Klassifizierung der Positivitätsbereiche ist auch für $n = 4$ noch relativ leicht möglich.

UNIVERSITÄT MÜNSTER/WESTF.

ON A PROBLEM OF WEYL IN THE THEORY OF SINGULAR STURM-LIOUVILLE EQUATIONS.*[1]

By N. ARONSZAJN.

1. In his famous paper [7] Weyl proposed the following problem: Consider the singular Sturm-Liouville equation

$$-(px')' + (q - \zeta)x = 0, \qquad 0 \leqq t < \infty, \tag{1.1}$$

with boundary condition at the regular endpoint $t = 0$

$$\sin\alpha\, x(0) - \cos\alpha\, p(0)x'(0) = 0. \tag{1.2$_\alpha$}$$

Suppose that the equation is in the limit-point case. Is the continuous spectrum preserved if the boundary condition (1.2_α) is changed into another, (1.2_β)?

A. Wintner stated a wider problem in a more general framework, namely, to investigate the changes in the spectrum of a self-adjoint problem when it is submitted to a one-dimensional perturbation (see P. Hartman [3]). Apparently very few papers have been published on this subject.[2] There is one by Putnam [5] which deals with the problem in its original setting.

Using a general theory of finite dimensional perturbations of spectral problems[3] the author was able to investigate the general problem of Wintner, showing in particular, that a one-dimensional perturbation can transform a pure point spectrum into a pure continuous spectrum and that for any self-adjoint spectral problem with simple spectrum, the part of the pure point spectrum contained in the limit spectrum can be made to disappear by a suitable one-dimensional perturbation. It was also proved that a part of the continuous spectrum, the *absolutely continuous spectrum*, is always preserved in finite dimensional perturbations. After these results were obtained, it became apparent that in the original setting of a singular Sturm-Liouville problem, most of these results could be achieved by using only the classical

---

* Received January 21, 1957.

[1] Written under contract with the Office of Naval Research, Contract Nonr 583(04).

[2] The author's attention was drawn to this problem in a conversation with P. Hartman.

[3] This theory will be presented in a paper by W. F. Donoghue and the author on "Finite dimensional perturbations of spectral problems and approximation methods."

background and recent results of Gelfand and Levitan [2]. This treatment of Weyl's problem in its original setting is the subject of the present paper.

In Section 2 we recall some properties of measures on the real axis and their relations to analytic functions in the upper half plane with positive imaginary part. In Section 3 we recall some essential facts from Weyl's theory of singular Sturm-Liouville equations and apply the developments of Section 2 to obtain our basic theorem concerning the conservation of the absolutely continuous spectrum (Theorem 1). In Section 4 we formulate an essential part of the basic result of Gelfand-Levitan [2] in a slightly improved form due to M. Krein [4]. From this result we deduce a sufficient condition for a measure μ to be equivalent to the spectral measure of a Sturm-Liouville problem in the limit-point case, with $p(t) \equiv 1$ (Theorem 2). This sufficient condition is used in the next sections to construct counter examples for Weyl's problem. In Section 5 we construct a Sturm-Liouville equation which for one boundary condition has a pure continuous singular spectrum concentrated on a closed set of Lebesgue measure 0 whereas for all other boundary conditions it has a pure point spectrum with all eigenvalues isolated. In Section 6 we give first a characterization of the point spectrum for a boundary condition (1.2_β) in terms of the spectral measure corresponding to another boundary condition, (1.2_α) (Theorem 4). Using this characterization we construct an example of a Sturm-Liouville problem which for one boundary condition has a pure point spectrum dense on the whole real axis, whereas for all other boundary conditions the spectrum is purely continuous.

2. We shall consider Lebesgue-Stieltjes measures on the real axis R; they will be given by a nondecreasing function $\mu(\lambda)$ normalized as follows: $\mu(0) = 0$, $\mu(\lambda) = \frac{1}{2}[\mu(\lambda+) + \mu(\lambda-)]$. The letters μ, ν, ρ, etc. will stand for the functions as well as the corresponding measures: $\mu(\lambda)$ is the value of the function at λ; $\mu(S)$ is the measure of the set S; $\mu\{\lambda\}$ is the measure of the set $\{\lambda\}$ composed of the single point λ, etc. The Lebesgue measure of a set S will be written $|S|$.

All notions relative to a measure when written without mention of the measure mean relative to the Lebesgue measure; for instance: a.e. (almost everywhere), absolutely continuous, etc.

A *support* of μ is a set S such that $\mu(R-S) = 0$. We recall that μ and ν are called *orthogonal* if some of their supports are disjoint.

The *closed support* of μ is the smallest among all closed sets which are supports of μ. Two equivalent measures have the same closed support;

the converse is not generally true. In our considerations the closed supports will not be the most important; we will not even require that a support be contained in the closed support. However, we will impose another restriction on supports (see (2.1) below).

A support S of μ is said to be *minimal rel.* ν if for any smaller support $S_1 \subset S$ of μ, $\nu(S - S_1) = 0$. It is clear that each support S of μ is minimal rel. μ and that two measures μ and ν are equivalent if and only if they have a common support which is minimal for each one of them rel. the other.

In accordance with our general convention we say that a support of μ is minimal if it is minimal rel. to the Lebesgue measure. From now on we will assume

(2.1) *All supports of measures will be assumed minimal.*

It follows that if S is a support of a singular measure, $|S| = 0$. Also if two absolutely continuous measures have the same support, they are equivalent.

For a point measure (i.e. a measure with an enumerable support) we will consider only the smallest support (i.e. the set of all points with positive measure).

Corresponding to a decomposition of μ into mutually orthogonal measures, ν_k, $\mu = \sum \nu_k$, we will consider supports S_k of ν_k as *admissible* if they are mutually disjoint. We are especially interested in the Lebesgue-Jordan (L.-J.) decompositions $\mu = \mu^0 + \mu^1$, $\mu^1 = \mu' + \mu''$, where μ^0 is the absolutely continuous part, μ^1 the singular part, μ' the singular continuous part, and μ'' the point measure corresponding to μ. Corresponding admissible supports for these decompositions can be obtained from a classical theorem of De la Vallée Poussin (see e.g. Saks [6]):

$$S^0{}_P = \mathop{\mathrm{E}}_{\xi}[d\mu(\xi)/d\lambda \text{ exists and } 0 < d\mu(\xi)/d\lambda < \infty],$$

$$S^1{}_P = \mathop{\mathrm{E}}_{\xi}[d\mu(\xi)/d\lambda \text{ exists and } d\mu(\xi)/d\lambda = \infty],$$

$$S''{}_P = S'' = \mathop{\mathrm{E}}_{\xi}[\mu(\lambda) \text{ is discontinuous at } \xi], \qquad S'{}_P = S^1{}_P - S''{}_P.$$

For our needs it will be more convenient to replace these supports by a slightly different system connected with analytic functions with positive imaginary part in the half-plane, $\operatorname{Im}\zeta > 0$. We recall some of the fundamental properties of these functions. Each such function $\phi(\zeta)$ has a canonical representation of the form

$$(2.2) \qquad \phi(\zeta) = \omega\zeta + \sigma + \int_{-\infty}^{\infty} [(\lambda - \zeta)^{-1} - \lambda(\lambda^2 + 1)^{-1}] d\mu(\lambda),$$

with $\omega \geqq 0$, σ real, and μ a positive measure such that

$$\int (\lambda^2+1)^{-1} d\mu < \infty. \tag{2.3}$$

Conversely, each choice of such ω, σ, and μ, defines by (2.2) a function $\phi(\zeta)$ with positive imaginary part for $\operatorname{Im}\zeta > 0$.

In the following properties we will use for a real ξ the expression "$\zeta \to \xi$ in an angle" meaning that for some ϵ, $0 < \epsilon < \frac{1}{2}\pi$, ζ converges to ξ remaining inside the angle $\epsilon < \operatorname{Arg}(\zeta - \xi) < \pi - \epsilon$. The statements below are well known.

I. *For* ξ *a. e. in* R, $\phi(\zeta)$ *converges to a finite limit when* $\zeta \to \xi$ *in any angle.*

II. *If* $d\mu(\xi)/d\lambda$ *exists (may be finite or infinite)* $\operatorname{Im}\phi(\lambda) \to \pi(d\mu(\xi)/d\lambda)$ *when* $\zeta \to \xi$ *in any angle.*

III. *If the upper derivative of* μ *at* ξ *is infinite, then* $\limsup_{\eta \searrow 0} \operatorname{Im}\phi(\xi + i\eta) = \infty$.

IV. *For every* ξ, $(\xi - \zeta)\phi(\zeta)$ *converges to* $\mu\{\xi\} = \mu(\xi+) - \mu(\xi-)$ *when* $\zeta \to \xi$ *in any angle.*

We now define our *standard* supports for the parts of μ in L.-J. decomposition as follows: We suppose that μ satisfies (2.3) and with any $\omega \geqq 0$ and σ real, we form the function $\phi(\zeta)$ by (2.2). We then put

$$S^0 = \mathop{\mathrm{E}}_{\xi}[\lim \phi(\zeta) \text{ exists and is finite and } \lim \operatorname{Im}\phi(\zeta) > 0 \text{ when } \zeta \to \xi \text{ in any angle}]. \tag{2.4^0}$$

$$S^1 = \mathop{\mathrm{E}}_{\xi}[\operatorname{Im}\phi(\zeta) \to \infty \text{ when } \zeta \to \xi \text{ in any angle}]. \tag{2.4^1}$$

$$S' = \mathop{\mathrm{E}}_{\xi}[\operatorname{Im}\phi(\zeta) \to \infty \text{ and } (\zeta - \xi)\phi(\zeta) \to 0 \text{ when } \zeta \to \xi \text{ in any angle}]. \tag{2.4$'$}$$

$$S'' = \mathop{\mathrm{E}}_{\xi}[\lim (\xi - \zeta)\phi(\zeta) > 0 \text{ when } \zeta \to \xi \text{ in any angle}]. \tag{2.4$''$}$$

That these are admissible supports follows immediately from the statements above by using the supports of de la Vallée Poussin. We have here $S^1 \supset S^1{}_P$, whereas there is no generally valid inclusion relation between S^0 and $S^0{}_P$.

It is obvious that the standard supports depend only on the measure and not on the choice of the constants ω and σ. It would be easy to define them without assuming the restriction (2.3) on μ but it is immaterial for us, since all the measures in which we are interested satisfy (2.3).

All the standard supports are contained in the closed support of μ but they are not necessarily contained in the closed supports of the corresponding parts of μ. It may even happen that the singular measure μ^1 is $=0$ with the support S^1 nonvanishing.

Remark. For two equivalent measures μ and ν the standard supports may be quite different. It can be proved quite easily, however, that if the derivative $d\mu(\lambda)/d\nu$ is given by a function $\tau(\lambda)$, continuous and positive on the whole real axis, and satisfying on each finite interval a Lipschitz condition, the standard supports for μ and ν are the same.

3. In the original setting for Weyl's treatment of equation (1.1) with boundary condition (1.2_α), it is assumed that $p(t)$ and $q(t)$ are continuous and $p(t)$ is positive for $0 \leqq t < \infty$. As usual, we form the solutions $\phi_\alpha(t,\zeta)$ and $\psi_\alpha(t,\zeta)$ of equation (1.1) determined by the initial values

$$\begin{aligned} &\phi_\alpha(0,\zeta) = \sin\alpha, \qquad \phi_\alpha'(0,\zeta)p(0) = -\cos\alpha, \\ &\psi_\alpha(0,\zeta) = \cos\alpha, \qquad \psi_\alpha'(0,\zeta)p(0) = \sin\alpha.^4 \end{aligned} \tag{3.1}$$

In the limit-point case there exists for each non-real ζ a unique complex number $m_\alpha(\zeta)$—the limit point—such that $\phi_\alpha(t,\zeta) + m_\alpha(\zeta)\psi_\alpha(t,\zeta)$ is in $L^2(0,\infty)$. It is known that $m_\alpha(\zeta)$ is analytic and with positive imaginary part in the half-plane $\operatorname{Im}\zeta > 0$. It is also proved that in the canonical representation of $m_\alpha(\zeta)$ of type (2.2), the constant $\omega = 0$. Hence

$$m_\alpha(\zeta) = \sigma_\alpha + \int_{-\infty}^{\infty} [(\lambda-\zeta)^{-1} - \lambda(\lambda^2+1)^{-1}]d\rho_\alpha(\lambda), \tag{3.2}$$

where the measure ρ_α satisfies condition (2.3).

The measure ρ_α is the Weyl spectral measure of the problem. Introducing the L.-J. decompositions of ρ_α, we get the traditional spectra defined as follows: The closed support of ρ_α is the spectrum of our problem; the support of ρ''_α is the point spectrum; the closed support of $\rho^0_\alpha + \rho'_\alpha$ is the continuous spectrum. The closed support of ρ_α minus all its isolated points (which belong to the point spectrum) forms the limit spectrum (sometimes called the essential spectrum). We may add here the absolutely continuous spectrum which is the closed support of ρ^0_α, and the singular continuous spectrum which is the closed support of ρ'_α.[5]

---

[4] The primes denote differentiation with respect to t.

[5] It is well known that these sets by themselves do not give an adequate representation of the spectral decomposition corresponding to the problem. It is rather the corresponding measures (or any measures equivalent to them) which should be considered as representing the spectra.

The function $m_\alpha(\zeta)$ and $m_\beta(\zeta)$ for two different boundary conditions satisfy the following relation, where we put $\gamma=\beta-\alpha$:

$$m_\beta(\zeta)=\{m_\alpha(\zeta)\operatorname{cotg}\gamma-1\}/\{m_\alpha(\zeta)+\operatorname{cotg}\gamma\}.^{6}$$

It will be more convenient for us to write this formula as follows:

$$(3.3)\qquad [m_\alpha(\zeta)+\operatorname{cotg}\gamma][m_\beta(\zeta)-\operatorname{cotg}\gamma]=-1/\sin^2\gamma.^{7}$$

We may define the standard supports $S^0{}_\alpha, S^1{}_\alpha,\cdots, S^0{}_\beta, S^1{}_\beta,\cdots$, for the L.-J. decompositions of ρ_α and ρ_β by using, for $\phi(\zeta)$, the functions $m_\alpha(\zeta)+\operatorname{cotg}\gamma$ and $m_\beta(\zeta)-\operatorname{cotg}\gamma$ respectively. A simple inspection of the definitions (2.4⁰) and (2.4¹) and formula (3.3) shows that $S^0{}_\alpha=S^0{}_\beta$ and that $S^1{}_\alpha\cap S^1{}_\beta=0$. Hence our theorem:

THEOREM 1. *For two distinct boundary conditions* (1.2_α) *and* (1.2_β) *the absolutely continuous parts of the corresponding spectral measures are equivalent, whereas the singular parts are orthogonal.*

This gives the positive part of our answer to Weyl's problem. The absolutely continuous spectrum does not change when the boundary condition is changed.

In the following sections we will construct examples showing that in general the singular continuous spectrum is not preserved.

Remark. In his paper, Putnam [5] proves the following statement: If in some open interval I, ρ_α is absolutely continuous relative to ρ_β for one $\beta\neq\alpha$, then it is absolutely continuous in I relative to $\rho_{\beta'}$ for all β'. From our theorem we can conclude more, namely: that under the hypothesis of Putnam, ρ_α in I is absolutely continuous and equivalent to the absolutely continuous part of $\rho_{\beta'}$ for all β'.

4. In order to construct the examples mentioned above, we need some information about sufficient conditions for a measure μ to be equivalent to a spectral measure of a singular Sturm-Liouville problem in the limit-point

---

[6] This formula can be found in the book of Coddington and Levinson [1], Exercise 8, page 257.

[7] In the general theory of perturbations of spectral problems (developed in the forthcoming paper of W. F. Donoghue and the author) where the change from one boundary condition to another takes the aspect of a one-dimensional perturbation, the two square brackets multiplied by ± sin γ are the determinants of the two opposite perturbations, and formula (3.3) is a special case of the general composition formula for the determinants of perturbations.

case. For this purpose we will recall briefly some recent results of Gelfand-Levitan [2] in an improved form due to Krein [4].

For a measure μ define the function $\sigma(\lambda)$ for $\lambda \geqq 0$

$$\sigma(\lambda) = \mu(\lambda) - 2\lambda^{\frac{1}{2}}/\pi, \textit{ for } \lambda \geqq 0. \tag{4.1}$$

Consider now the following conditions:

(4.2) *The closed support of μ possesses a finite limit point.*

(4.3) *For some $\theta < 2$, $\int_{-\infty}^{0} \exp\{(-\lambda)^{\frac{1}{2}}t\}d\mu(\lambda) < \exp(t^{\theta})$ for sufficiently large positive t.*

(4.4_k) *The integral $\int_{1}^{\infty} \lambda^{-1}\cos(\lambda^{\frac{1}{2}}t)\,d\sigma(\lambda)$ is absolutely convergent for all $0 \leqq t < \infty$ and defines a function $a(t)$ with continuous $k+3$ derivatives.*

THEOREM OF GELFAND-LEVITAN. *If $\mu(\lambda)$ satisfies the conditions* (4.2), (4.3), *and* (4.4_k) *for some $k = 0, 1, 2, \cdots$ then μ is the Weyl spectral measure ρ_α for a uniquely determined Sturm-Liouville problem $-x'' + (q - \zeta)x = 0$, $x'(0) = \tan\alpha\, x(0)$ where $-\frac{1}{2}\pi < \alpha < \frac{1}{2}\pi$, $q(t)$ has k continuous derivatives and the problem is in the limit-point case.*

Remark 1. From the relation between $a(t)$ and $q(t)$ (given by Gelfand and Levitan [2]) it follows easily that if $a(t)$ is analytic in the real variable t for $0 \leqq t < \infty$, then so is also the function $q(t)$.

We can now give sufficient conditions for a measure μ to be equivalent to a spectral measure of a singular Sturm-Liouville problem in the limit point case.

THEOREM 2. *Let μ be a measure satisfying* (4.2) *and let $\{\xi_l\}$, $l = 0, 1, 2, \cdots$, be a strictly increasing sequence such that $\xi_0 = 0$, $\xi_1 \geqq 1$, $\xi_l \to \infty$, $\mu\{\xi_l\} = 0$ for $l \geqq 1$, and $\mu(\xi_{l+1}) - \mu(\xi_l) > 0$ for all l. If for some $k \geqq 0$, the condition*

$$\sum_{l=1}^{\infty} \xi_l^{\frac{1}{2}(k-1)}(\xi_{l+1} - \xi_l)^2 < \infty \tag{4.5}$$

is satisfied, there exists a measure ρ equivalent to μ such that ρ is the spectral measure ρ_α of a Sturm-Liouville problem in the limit-point case, with $p(t) = 1$, $q(t)$ k times continuously differentiable and $-\frac{1}{2}\pi < \alpha < \frac{1}{2}\pi$. In addition, for each bounded part of a support of μ there exist constants C_0 and C_1 such that $0 < C_0 < d\rho/d\mu < C_1 < \infty$.

Proof. We construct a measure ρ equivalent to μ and which satifies the conditions in the Gelfand-Levitan theorem. Obviously, for every ρ equivalent to μ (4. 2) is satisfied. In order to fulfill condition (4. 3) we proceed as follows. In each open interval $(-n; -n+1)$, for $n = 1, 2, \cdots$ we put $d\rho(\lambda) = \exp(-\lambda^2)[\mu(-n+1) - \mu(-n)]^{-1} d\mu(\lambda)$ unless there is no measure in this interval, in which case we put $d\rho(\lambda) = 0$. For each $n = 1, 2, \cdots$, for which $\mu\{-n\} > 0$, we put $\rho\{-n\} = \exp(-n^2)$; if $\mu\{-n\} = 0$, we put $\rho\{-n\} = 0$. It is easy to check that ρ so defined on the left axis is equivalent there to μ, satisfies condition (4. 3), and also the last condition in the theorem.

We define now the measure ρ on the half axis $\lambda \geqq 0$ by putting $\rho\{0\} = [2\xi_1^{\frac{1}{2}}/\pi\mu(\xi_1)]\mu\{0\}$ and on each interval

$$(\xi_l; \xi_{l+1}] : d\rho(\lambda) = 2\pi^{-1}[\xi_{l+1}^{\frac{1}{2}} - \xi_l^{\frac{1}{2}}][\mu(\xi_{l+1}) - \mu(\xi_l)]^{-1} d\mu(\lambda).$$

$\rho(\lambda)$ defined in this way on the positive axis is obviously equivalent to μ and satisfies the last condition in the theorem. Also like $\mu(\lambda)$, $\rho(\lambda)$ is continuous at the points ξ_l, $l \geqq 1$.

To prove condition (4. 4_k) consider for $\lambda \geqq 0$, $\sigma(\lambda) = \rho(\lambda) - 2\pi^{-1}\lambda^{\frac{1}{2}}$. Since $\rho(\xi_0) = \rho(0) = 0$ and $\rho(\xi_{l+1}) - \rho(\xi_l) = 2\pi^{-1}[\xi_{l+1}^{\frac{1}{2}} - \xi_l^{\frac{1}{2}}]$ we have $\sigma(\xi_l) = 0$ for all l.

We show first that the integral defining $a(t)$ is absolutely convergent. In fact

$$\int_1^\infty \lambda^{-1} \,|\, d\sigma(\lambda) | = \int_1^{\xi_1} \lambda^{-1} \,|\, d\sigma(\lambda) | + \sum_{l=1}^{\infty} \int_{\xi_l}^{\xi_{l+1}} \lambda^{-1} \,|\, d\sigma(\lambda) |,$$

$$\int_{\xi_l}^{\xi_{l+1}} \lambda^{-1} \,|\, d\sigma(\lambda) | \leqq 2\pi^{-1} \int_{\xi_l}^{\xi_{l+1}} \lambda^{-1} d\lambda^{\frac{1}{2}} + 2\pi^{-1}[\xi_{l+1}^{\frac{1}{2}} - \xi_l^{\frac{1}{2}}][\mu(\xi_{l+1}) - \mu(\xi_l)]^{-1}$$

$$\times \int_{\xi_1}^{\xi_{l+1}} \lambda^{-1} d\mu(\lambda) \leqq 2\pi^{-1} \left\{ \int_{\xi_l}^{\xi_{l+1}} \lambda^{-1} d\lambda^{\frac{1}{2}} + \xi_l^{-1}[\xi_{l+1}^{\frac{1}{2}} - \xi_l^{\frac{1}{2}}] \right\}.$$

Condition (4. 5) implies that there exists a constant c such that $\xi_{l+1} < c\xi_l$, $l \geqq 1$. It follows that the last expression is majorated by $2(1+c)\pi^{-1} \int_{\xi_1}^{\xi_{l+1}} \lambda^{-1} d\lambda^{\frac{1}{2}}$ and hence

$$\int_1^\infty \lambda^{-1} \,|\, d\sigma(\lambda) | \leqq \int_1^{\xi_1} \lambda^{-1} \,|\, d\sigma(\lambda) | + 2(1+c)\pi^{-1} \int_{\xi_1}^{\infty} \lambda^{-1} d\lambda^{\frac{1}{2}} < \infty.$$

Next we express $a(t)$ as follows

$$a(t) = \int_1^{\xi_1} \lambda^{-1} \cos(\lambda^{\frac{1}{2}} t) \, d\sigma(\lambda) + \sum_{l=1}^{\infty} \int_{\xi_l}^{\xi_{l+1}} \lambda^{-1} \cos(\lambda^{\frac{1}{2}} t) \, d\sigma(\lambda) = u_0(t) + \sum_{l=1}^{\infty} u_l(t).$$

To prove condition (4.4_k) it is now sufficient to show that the $(k+3)$-th derivatives of $u_l(t)$ form an absolutely and uniformly convergent series in every finite interval of the variable t.

By partial integration and using the fact that $\sigma(\xi_l)=0$, we get

$$|u_l^{(k+3)}(t)| = \left|\int_{\xi_l}^{\xi_{l+1}} \lambda^{\frac{1}{2}(k+1)} \begin{matrix}\cos\\ \sin\end{matrix}(\lambda^{\frac{1}{2}}t)\,d\sigma(\lambda)\right|$$

$$= \left|\int_{\xi_l}^{\xi_{l+1}} [\tfrac{1}{2}(k+1)\lambda^{\frac{1}{2}(k-1)} \begin{matrix}\cos\\ \sin\end{matrix}(\lambda^{\frac{1}{2}}t) \mp \tfrac{1}{2}t\lambda^{\frac{1}{2}k} \begin{matrix}\sin\\ \cos\end{matrix}(\lambda^{\frac{1}{2}}t)]\sigma(\lambda)\,d\lambda\right|.$$

In the interval $(\xi_l;\xi_{l+1}]$ we have

$$|\sigma(\lambda)| = |\sigma(\lambda)-\sigma(\xi_l)|$$

$$\leqq \max\{2\pi^{-1}[\lambda^{\frac{1}{2}}-\xi_l^{\frac{1}{2}}],\,[\rho(\lambda)-\rho(\xi_l)]\} \leqq 2\pi^{-1}[\xi_{l+1}^{\frac{1}{2}}-\xi_l^{\frac{1}{2}}],$$

hence by using $\xi_{l+1}<c\xi_l$ we get the evaluation

$$|u_l^{(k+3)}(t)| \leqq \tfrac{1}{2\pi}c^{\frac{1}{2}k}(t+k+1)\xi_l^{\frac{1}{2}(k-1)}(\xi_{l+1}-\xi_l)^2.$$

Reference to (4.5) finishes the proof.

Remark 2. It is clear from the proof that the sum in (4.5) essentially bounds the $(k+3)$-th derivative of $a(t)$. Again, by using the relations between $q(t)$ and $a(t)$ we obtain the following statements: if the sum is finite for all k, $a(t)$ and $q(t)$ are of class C^∞; if the sums are bounded by $CM^kk!$, $a(t)$ and $q(t)$ are analytic.

Condition (4.5) will be the one to be used in our examples. It is of interest however to replace it by a condition more directly connected with the structure of the measure μ.

Let $(\lambda_i;\lambda'_i)$ be all the component intervals of $(1;\infty)-S$ where S is the closed support of μ.

THEOREM 3. *The existence of a sequence $\{\xi_l\}$ satisfying the requirements of Theorem 2 is equivalent to the condition*

$$\sum_i \lambda_i^{\frac{1}{2}(k-1)}(\lambda'_i-\lambda_i)^2<\infty. \tag{4.6}$$

Proof. Necessity of (4.6). Since the intervals $(\lambda_i;\lambda'_i)$ cannot contain any of the intervals $(\xi_l;\xi_{l+1}]$, each of the former must be contained in one of the latter or in the union of two consecutive intervals of the latter kind. If $\sum^{(l)}$ denotes summation over all i such that $(\lambda_i;\lambda'_i)\subset(\xi_l;\xi_{l+2}]$ we get for $l\geqq 1$ (constant c satisfying $\xi_{l+1}\leqq c\xi_l$)

$$\begin{aligned}\sum\nolimits^{(l)} \lambda_i^{\frac{1}{2}(k-1)}(\lambda'_i-\lambda_i)^2 &\leqq c^{k-1}\xi_l^{\frac{1}{2}(k-1)}(\xi_{l+2}-\xi_l)^2\\ &\leqq 2c^{k-1}[\xi_l^{\frac{1}{2}(k-1)}(\xi_{l+1}-\xi_l)^2+\xi_{l+1}^{\frac{1}{2}(k-1)}(\xi_{l+2}-\xi_{l+1})^2],\\ \sum\nolimits^{(0)} \lambda_i^{\frac{1}{2}(k-1)}(\lambda'_i-\lambda_i)^2 &\leqq \xi_2^{\frac{1}{2}(k+3)}.\end{aligned}$$

By adding up these inequalities we obtain (4.6) from (4.5).

Sufficiency of (4.6). We choose a sequence $\{\eta_l\}$ satisfying all the conditions of Theorem 2 (when ξ_l is replaced by η_l) except perhaps the condition $\mu(\eta_{l+1})-\mu(\eta_l)>0$. This is obviously always possible.[8]

We arrange the sequence of intervals $(\eta_n;\eta_{n+1}]$ into successive groups of consecutive intervals so that the total measure μ of each group be positive. We define these groups successively, each time choosing the *smallest* group with positive total measure. All the groups are finite (because of (4.6)) and hence they form consecutive intervals $(\eta_{n_l};\eta_{n_{l+1}}]$, $l=0,1,2,\cdots$, with the following properties: 1°: n_l are strictly increasing integers, $n_0=0$, $\eta_{n_1}\geqq 1$; 2°: if $n_{l+1}-1>n_l$ and $l\geqq 1$, there exists an interval $(\lambda_{i_l};\lambda'_{i_l})$ such that $\eta_{n_l-1}<\lambda_{i_l}\leqq\eta_{n_l}<\eta_{n_{l+1}-1}\leqq\lambda'_{i_l}<\eta_{n_{l+1}}$. We now put $\xi_l=\eta_{n_l}$. If $n_{l+1}-1=n_l$ then the term $\xi_l^{\frac{1}{2}(k-1)}(\xi_{l+1}-\xi_l)^2$ is part of the sum (4.5) written for η_l and the sum of these terms is finite. If $n_{l+1}-1>n_l$, $l\geqq 1$, then by 2°: $\xi_l^{\frac{1}{2}(k-1)}(\xi_{l+1}-\xi_l)^2\leqq\eta_{n_l}^{\frac{1}{2}(k-1)}2[(\lambda'_{i_l}-\lambda_{i_l})^2+(\eta_{n_{l+1}}-\eta_{n_{l+1}-1})^2]$. Since (4.6) implies that for some constant c_1, $\lambda'_i\leqq c_1\lambda_i$ it follows that

$$\xi_l^{\frac{1}{2}(k-1)}(\xi_{l+1}-\xi_l)^2\leqq 2c_1^{\frac{1}{2}(k-1)}\lambda_{i_l}^{\frac{1}{2}(k-1)}(\lambda'_{i_l}-\lambda_{i_l})^2+2\eta_{n_{l+1}-1}^{\frac{1}{2}(k-1)}(\eta_{n_{l+1}}-\eta_{n_{l+1}-1})^2;^{9}$$

hence the sum of these terms is again finite by (4.6) and by (4.5) written for η_l. Thus (4.5) is proved for $\{\xi_l\}$ and obviously this sequence satisfies all the other conditions of Theorem 2.

Remark 3. The preceding proof can be extended easily to prove that the sum (4.6) admits of a majoration $CM^kk!$ if and only if there exists a sequence ξ_l satisfying the conditions of Theorem 2 such that a similar majoration of the sum (4.5) is true.

5. We construct the first example announced in Section 1. Consider a sequence $\{\xi_l\}$ defined for all integers l with $-N<l<\infty$ and $0\leqq N\leqq\infty$.

---

[8] For instance for a suitable $\tau>(\log 2)^{-1}$, we can put $\eta_l=\tau\log(l+1)$. For this choice $\sum\eta_l^{\frac{1}{2}(k-1)}(\eta_{l+1}-\eta_l)^2$ is finite for all k and of order of magnitude $C_\epsilon\epsilon^kk!$ for all $\epsilon>0$ and suitable constants C_ϵ.

[9] This evaluation is valid for $k\geqq 1$. For $k=0$ it is obvious how it should be changed.

We suppose that $\xi_l < \xi_{l+1}$ for all l, $\xi_1 > 1$, and that $\xi_l \to \infty$ when $l \to \infty$, and finally that

$$(5.1) \qquad \sum_1^\infty \xi_l^{-\frac{1}{2}} (\xi_{l+1} - \xi_l)^2 < \infty.$$

In each interval $(\xi_l ; \xi_{l+1})$ take a closed set S_l dense in itself, with $|S_l| = 0$. We define a Sturm-Liouville problem $-x'' + (q - \zeta)x = 0$ with boundary condition $x'(0) = \operatorname{tang}\alpha\, x(0)$, with continuous $q(t)$, and $-\frac{1}{2}\pi < \alpha < \frac{1}{2}\pi$, such that the spectral measure ρ_α is a pure singular continuous measure with support $S = \cup S_l$. This problem will be such that for any other boundary condition with $\beta \neq \alpha \bmod \pi$, ρ_β will be a pure point measure concentrated on isolated points in the complement of S. To this effect we first construct for each S_l a continuous singular measure μ_l with support S_l such that for each $\xi \in S_l$ the upper derivative of μ_l at ξ is $= \infty$. It is well known that such measures exist.

We then define $\mu = \sum \mu_l$. It is clear that for support, μ has the set $S = \cup S_l$ and that for each $\xi \in S$, $\bar{d}\mu(\xi)/d\lambda = \infty$. If we now construct, as in Theorem 2, the measure $\rho = \rho_\alpha$ and the corresponding Sturm-Liouville problem, the measure ρ_α will be pure continuous singular with support S and $\bar{d}\rho_\alpha(\xi)/d\lambda = \infty$ for each $\xi \in S$.

Consider now any $\beta \neq \alpha \bmod \pi$ and apply statement III of Section 2 to $m_\alpha(\zeta) + \operatorname{cotg}\gamma$, where $\gamma = \beta - \alpha$. We see that

$$\limsup_{\eta \searrow 0} \operatorname{Im}[m_\alpha(\xi + i\eta) + \operatorname{cotg}\gamma] = \infty$$

for every $\xi \in S$. It follows from formula (3.3) that

$$\liminf_{\eta \searrow 0} | m_\beta(\xi + i\eta) - \operatorname{cotg}\gamma | = 0$$

for $\xi \in S$. By definitions (2.4^0) and (2.4^1) supports $S^0{}_\beta$ and $S^1{}_\beta$ are disjoint from S. From Theorem 1 we know that $S^0{}_\beta = 0$ and hence $S^1{}_\beta$ is the whole support of the measure ρ_β and lies in the complement of S. But on this complement the function $m_\alpha(\zeta) + \operatorname{cotg}\gamma$ is analytic and real with simple zeros, one at most in each of the components of the complement of S. Hence $S^1{}_\beta$ is the set of all zeros of $m_\alpha(\zeta) + \operatorname{cotg}\gamma$ in the complement of S. This proves all our assertions.

Remark. If we choose the sequence ξ_l so that $\sum_1^\infty \xi_l^{\frac{1}{2}(k-1)} (\xi_{l+1} - \xi_l)^2$ be finite for some $k \geqq 1$, or finite for all $k \geqq 0$ and majorated by $CM^k k!$, we would get in our example $q(t)$ k-times continuously differentiable, or analytic, respectively.

6. Before we construct the second example we prove the following theorem

THEOREM 4. *Consider the Sturm-Liouville equation* (1.1) *and two boundary conditions corresponding to* $\alpha \neq \beta \bmod \pi$, $\gamma = \beta - \alpha$. *In order that* ξ *be in the point spectrum relative to the boundary condition* (1.2_β) *it is necessary and sufficient that* $\int_{-\infty}^{\infty} (\lambda - \xi)^{-2} d\rho_\alpha(\lambda) < \infty$ *and that* $m_\alpha(\xi) + \operatorname{cotg}\gamma = 0$.

Proof. By statement IV in Section 2 we know that for the point ξ to have a positive mass $\rho_\beta\{\xi\}$ it is necessary and sufficient that

$$\lim (\xi - \zeta)[m_\beta(\zeta) - \operatorname{cotg}\gamma] = \rho_\beta\{\xi\}$$

when $\zeta \to \xi$ in any angle. By (3.3) this condition is equivalent to

$$\lim (\zeta - \xi)^{-1}[m_\alpha(\zeta) + \operatorname{cotg}\gamma] = [\sin^2 \gamma \rho_\beta\{\xi\}]^{-1} < \infty.$$

In the last equation put $\zeta = \xi + i\eta$, $\eta \searrow 0$. Using the expression (3.2) we obtain

$$\operatorname{Re}[(i\eta)^{-1}\{\operatorname{cotg}\gamma + \sigma_\alpha + \int_{-\infty}^{\infty} [(\lambda - \xi - i\eta)^{-1} - \lambda(\lambda^2 + 1)^{-1}] d\rho_\alpha(\lambda)\}]$$
$$= \int [(\lambda - \xi)^2 + \eta^2]^{-1} d\rho_\alpha(\lambda).$$

The last integrand is a decreasing function of η for each λ and it follows that for $\eta \searrow 0$ the integral converges to $\int (\lambda - \xi)^{-2} d\rho_\alpha(\lambda)$. Thus we get

$$\int (\lambda - \xi)^{-2} d\rho_\alpha(\lambda) = [\sin^2 \gamma \rho_\beta\{\xi\}]^{-1} < \infty.$$

It follows further that

$$\lim_{\eta \searrow 0} \{\operatorname{cotg}\gamma + \sigma_\alpha + \int [(\lambda - \xi - i\eta)^{-1} - \lambda(\lambda^2 + 1)^{-1}] d\rho_\alpha(\lambda)\}$$
$$= \operatorname{cotg}\gamma + \sigma_\alpha + \int [(\lambda - \xi)^{-1} - \lambda(\lambda^2 + 1)^{-1}] d\rho_\alpha(\lambda) = 0.$$

This gives the necessity of our conditions. If the conditions are satisfied, then by the last equation we can write

$$\operatorname{cotg}\gamma + m_\alpha(\zeta) = \int [(\lambda - \zeta)^{-1} - (\lambda - \xi)^{-1}] d\rho_\alpha(\lambda)$$
$$= (\zeta - \xi) \int [1/(\lambda - \zeta)(\lambda - \xi)] d\rho_\alpha(\lambda).$$

In view of our conditions, the quotient of this expression by $(\zeta-\xi)$ converges to $\int(\lambda-\xi)^{-2}d\rho_\alpha(\lambda)$ when $\zeta\rightarrow\xi$ in any angle. Then by reversing the previous argument we arrive at the conclusion that ρ_β has a positive mass at the point ξ.

In our next example we choose an arbitrary enumerable set S dense on the whole real axis and construct a Sturm-Liouville problem such that for one α, ρ_α is a pure point measure with support S, whereas for all $\beta\neq\alpha \bmod \pi$, ρ_β will be a pure singular continuous measure. To this effect we will assign to each $\xi\in S$ a positive measure $\mu\{\xi\}$ in such a way that the total measure in any finite interval be finite, and for each real ξ the quotient $\mu(I)/|I|^2\rightarrow\infty$ for at least one sequence of intervals I containing ξ and converging to ξ. If this condition is satisfied then obviously for each ξ we have $\int(\lambda-\xi)^{-2}d\mu(\lambda)=\infty$ and this will be true also for the equivalent measure $\rho=\rho_\alpha$ defined in Theorem 2 (by virtue of the last assertion in this theorem). Therefore by Theorem 4, for all $\beta\neq\alpha \bmod \pi$ there cannot be any point spectrum. On the other hand, there cannot be any absolutely continuous spectrum since there is none for ρ_α (see Theorem 1). Hence ρ_β is a pure continuous singular measure.

There remains the construction of the measure μ. We define it in each of the intervals $(l;l+1]$. Since the construction is completely similar in each interval we shall do it only for $(0;1]$. We consider consecutive subdivisions of the interval in 2^k subintervals, $I_{k,i}=(2^{-k}(i-1);2^{-k}i]$, $i=1,2,\cdots,2^k$, $k=1,2,3,\cdots$. To each subinterval we assign a point $\xi_{k,i}\in S\cap I_{k,i}$ in the following way. We consider the points of S as arranged in a simple sequence, $\eta_1,\eta_2,\cdots$. To each of the intervals $I_{1,i}$ we assign the first element of the sequence $\{\eta_n\}$ which lies in this interval. If the $\xi_{k,i}$ are already defined for all $k<k_0$, we define $\xi_{k_0,i}$ as the first element in $\{\eta_n\}$ which lies in $I_{k_0,i}$ and which was not assigned to any previous interval. It is clear that in this way we will assign points $\xi_{k,i}$ to all intervals $I_{k,i}$ and the set of all $\xi_{k,i}$ is exactly equal to $S\cap(0;1]$. To the points $\xi_{k,i}$ we assign the measure $\mu\{\xi_{k,i}\}=3^{-k}$. The total measure for the interval $(0;1]$ is then $\sum_1^\infty(2/3)^k=2$.

Consider now any point ξ with $0<\xi\leqq 1$ and the sequence of intervals I_{k,i_k} containing ξ. We have $\mu(I_{k,i_k})>\mu\{\xi_{k,i_k}\}=3^{-k}$, $|I_{k,i_k}|=2^{-k}$, hence $\mu(I_{k,i_k})/|I_{k,i_k}|^2>(4/3)^k\rightarrow\infty$ which finishes the proof.

Remark. Since in the above example, there are no intervals with μ-

measure 0, the developments of Section 4 allow us to construct a corresponding Sturm-Liouville problem with an analytic function $q(t)$.

University of Kansas.

REFERENCES.

[1] E. A. Coddington and N. Levinson, *Theory of ordinary differential equations*, McGraw-Hill, New York, 1955.

[2] I. M. Gelfand and B. M. Levitan, "Determination of a differential equation by its spectral function," *Izviestia Ak. N. SSSR S. M.*, vol. 15 (1951), pp. 309-360.

[3] P. Hartman, "On the essential spectra of symmetric operators in Hilbert space," *American Journal of Mathematics*, vol. 75 (1953), pp. 229-240.

[4] M. Krein, "On a method of effective solution of an inverse boundary problem," *Dokl. Ak. N. SSSR*, vol. 94 (1954), pp. 987-990.

[5] C. R. Putnam, "On the continuous spectra of singular boundary value problems," *Canadian Journal of Mathematics*, vol. 6 (1954), pp. 420-426.

[6] S. Saks, *Theory of the Integral*, Warsaw-Lwow, 1937.

[7] H. Weyl, "Über gewöhnliche Differentialgleichungen mit Singularitäten . . .," *Mathematische Annalen*, vol. 68 (1910), pp. 222-269.

CHARACTERIZATION OF POSITIVE REPRODUCING KERNELS. APPLICATIONS TO GREEN'S FUNCTIONS.*[1]

By N. Aronszajn and K. T. Smith.

1. Introduction. The object of this paper is to prove a theorem which characterizes the proper functional Hilbert spaces whose reproducing kernels are positive. Since certain Green's functions are among the most important examples of reproducing kernels, it is natural that the general theorem leads to results about the positiveness of Green's functions.

Not all Green's functions are reproducing kernels; those and only those are which correspond to positive definite differential problems of sufficiently high order. This restriction on the order is avoided by use of the notion of pseudo-reproducing kernels for general Hilbert spaces. Details of the underlying theory of pseudo-reproducing kernels are not given, except for those basic definitions and properties which are necessary to make clear the application of the abstract theorem about positiveness.

Roughly speaking[2] in the case of a self-adjoint elliptic problem, the Green's function exists if the problem is well posed, i.e., if there exists no solution to the homogeneous equation satisfying the homogeneous boundary conditions (in other words if 0 is not an eigenvalue of the corresponding eigenvalue problem).[3] A Green's function exists and is a reproducing or pseudo-reproducing kernel if and only if the problem is definite positive (i.e., if all the eigenvalues are positive). Our abstract theorem about reproducing kernels gives necessary and sufficient conditions in order that a Green's function corresponding to a *positive definite problem* be positive. We do not know if there exist positive Green's functions corresponding to problems which are not positive definite.

In the case of second order problems the question of which Green's functions are positive is answered completely by a proof of the equivalence of the following statements: (i) the problem is positive definite and (ii) the

---

* Received January 21, 1957.

[1] Paper written under contract with the Office of Naval Research Nonr 583(04).

[2] The additional restrictions under which the following statements can actually be proved are stated in Section 4.

[3] This excludes from our considerations the Neumann function for $\Delta u = 0$; this function actually changes sign in the domain.

Green's function exists and is positive. In the case of higher order problems there are examples showing that (ii) does not follow from (i) even in case of the square of the Laplacian and the boundary conditions $u = \partial u/\partial n = 0$.[4] However, we give examples of fourth order problems where it can be proved by the abstract theorem that the Green's function is positive, and where a simple direct proof does not seem to lie near at hand. The results are not restricted to problems about domains in Euclidean space. They are stated and proved for problems about relatively compact domains in oriented differentiable manifolds.

The question of positiveness of Green's functions is a very old one. For special cases like the Laplace equation with Dirichlet boundary condition, it goes back to the classical papers of C. Neumann and H. A. Schwarz where the positiveness of the Green's function is an important tool in investigations. Since then the positiveness of the Green's function was proved by many authors in many special cases of second order problems. Since for such problems with Dirichlet boundary condition the positiveness of the Green's function is closely related with the maximum principle, we should mention here the work of E. Hopf [12] who investigated this principle for the most general second order equations. It would seem that the first formal recognition of the relation between the positiveness of the Green's function and the positive character of the differential problem of second order with the Dirichlet boundary condition can be found in the thesis of Bleuler [13].

Our results on second order problems include as quite special cases some of the results of Bergman and Schiffer [6],[5] and can be proved, in a heuristic manner at least, by following the lines set forth by Bergman and Schiffer in the special cases. The difficulty in this approach lies in the lack of general information about the sets of points on which solutions to the differential equation are zero. Our method does not require information of this kind.

2. Reproducing kernels. The main theorem of the paper, Theorem 1 below, gives necessary and sufficient conditions in order that the reproducing kernel $K(x,y)$ of a proper functional Hilbert space be non-negative.[6] It is proved in [2] that condition (a) in the theorem below is necessary and sufficient in order that $K(x,y)$ be real.[7]

---

[4] The problem of positiveness of the corresponding Green's function in case of two variables is the famous problem of Hadamard stated in the first decade of this century and solved negatively less than ten years ago by Duffin [7] and Garabedian [8].

[5] These authors consider only the differential operator $-\Delta + p$, $p > 0$, and consider boundary conditions slightly more special than ours; they consider explicitly only the case of 2 variables. However, they treat two questions related to the question treated here; when a Green's function is positive, and when one Green's function is larger than another. The second question is not discussed in this paper, but will be discussed from a similar general point of view in another paper.

THEOREM 1. *In order that the reproducing kernel* $K(x,y)$ *of the proper functional Hilbert space* $\mathfrak{F}$ *be non-negative it is necessary and sufficient that* $\mathfrak{F}$ *have the two properties*

(a) *If* $u \in \mathfrak{F}$, *then* $\bar{u} \in \mathfrak{F}$ *and* $\| \bar{u} \| = \| u \|$.

(b) *For each real-valued* $u \in \mathfrak{F}$ *there exists* $\tilde{u} \in \mathfrak{F}$ *such that*

$$\tilde{u}(x) \geqq | u(x) | \text{ for all } x \text{ and } \| \tilde{u} \| \leqq \| u \|.$$

Proof. Assuming that $\mathfrak{F}$ has the properties (a) and (b), let $u \in \mathfrak{F}$, u be real-valued and let $\tilde{u}$ be such that (b) holds, and set $u^+ = \frac{1}{2}(\tilde{u} + u)$ and $u^- = \frac{1}{2}(\tilde{u} - u)$. Clearly u^+ and u^- are both non-negative, and $\tilde{u} = u^+ + u^-$ and $u = u^+ - u^-$. By using (a) it is proved easily that the scalar product of real-valued functions is real. Therefore, from $\| \tilde{u} \| \leqq \| u \|$ it follows that $(u^-, u^+) \leqq 0$, and hence that $(u^-, u) = (u^-, u^+) - (u^-, u^-) \leqq - \| u^- \|^2$. By virtue of the result from [2] quoted above, $K_y(x) = K(x,y)$ is real-valued for every y so that this inequality can be applied to $u = K_y$ to give $0 \leqq K_y^-(y) = (K_y^-, K_y) \leqq - \| K_y^- \|^2$. This is possible only if $K_y^- = 0$ so that $K_y = K_y^+ \geqq 0$.

Assuming that $K(x,y) \geqq 0$, for each real-valued $u \in \mathfrak{F}$, let u' and u'' be the projections of u and of $-u$ on the closed convex cone with vertex 0 generated by the set $\{K_y\}$. Then for every $\rho \geqq 0$ and every v in the cone, $\| u - u' \|^2 \leqq \| u - u' - \rho v \|^2$, from which it follows that for every v in the cone $(u' - u, v) \geqq 0$. Applying this to $v = K_y$, we obtain $u'(y) \geqq u(y)$ for every y. Similarly, $u''(y) \geqq -u(y)$ for every y. Since $K(x,y)$ is non-negative, both u' and u'' are non-negative, so that if $\tilde{u} = u' + u''$, then $\tilde{u}(x) \geqq | u(x) |$ for all x. All that remains is to show that $\| \tilde{u} \| \leqq \| u \|$. This was done in another paper [5], but since the proof is very short it bears repetition.

---

[6] A proper functional Hilbert space is a Hilbert space whose elements are functions on a basic set $\mathcal{E}$, such that the value of a function at any point in $\mathcal{E}$ is a continuous linear functional. To each proper functional Hilbert space $\mathcal{F}$ there corresponds a function $K(x,y)$, called the reproducing kernel of $\mathcal{F}$, defined on $\mathcal{E} \times \mathcal{E}$ and having the properties:

(a) for each $y \in \mathcal{E}$, the function $K_y(x) = K(x,y)$ belongs to $\mathcal{E}$.

(b) the reproducing property: for each $u \in \mathcal{F}$, $u(y) = (u, K_y)$.

[7] If u is a complex valued function, $\bar{u}$ is its complex conjugate; i.e., $\bar{u}(x)$ is the complex conjugate of $u(x)$.

If ϕ', α, and ϕ'' are the angles between u and u', u' and u'', and u'' and $-u$, respectively, then, as $u-u'$ is orthogonal to u' and $-u-u''$ is orthogonal to u'', the inequality to be proved takes the form

$$\| u \|^2 (\cos^2 \phi' + \cos^2 \phi'' + 2\cos \phi' \cos \phi'' \cos \alpha) \leqq \| u \|^2,$$

which is easy to establish with the aid of the inequalities $0 \leqq \phi' \leqq \frac{\pi}{2}$, $0 \leqq \phi'' \leqq \frac{\pi}{2}$, and $\pi \leqq \phi' + \alpha + \phi''$.

Remark 1. If condition (a) holds for a set of functions which is dense in $\mathfrak{F}$, then condition (a) holds for all function in $\mathfrak{F}$. If condition (b) holds for a set of functions which is dense in the set of all real-valued functions in $\mathfrak{F}$, then condition (b) holds for all real-valued functions in $\mathfrak{F}$.

Remark 2. The following statement about matrices is a consequence of Theorem 1. *Let $\{a_{ij}\}$ be a real positive definite matrix. In order that every element in $\{a_{ij}\}^{-1}$ be non-negative it is necessary and sufficient that for each real vector u there exist $\tilde{u}$ such that $\tilde{u}_i \geqq | u_i |$ for all i and $\sum a_{ij}\tilde{u}_i\tilde{u}_j \leqq \sum a_{ij}u_iu_j$.*

3. Pseudo-reproducing kernels. The functional spaces which are of use in differential problems are proper functional Hilbert spaces in problems of order larger than the dimension of the underlying Euclidean space. In problems of smaller order the spaces are more general functional Hilbert spaces in which the functions are not defined everywhere.

A functional space is a normed linear class $\mathfrak{F}$ of functions on a basic set $\mathcal{E}$, each defined except on some exceptional set belonging to a hereditary σ-ring $\mathfrak{A}$ (the exceptional class of sets). It is assumed that the norm in $\mathfrak{F}$ has the property that if $\| u_n - u \| \to 0$, then, for some subsequence $\{u_{n_k}\}$, $u_{n_k}(x) \to u(x)$ except on a set in $\mathfrak{A}$. A complete discussion of functional spaces and functional completion can be found in [5].

Let μ be a σ-finite complete measure on a set $\mathcal{E}$. The class of measurable subsets of $\mathcal{E}$ of finite measure will be denoted by $\mathcal{E}'$, the sets in $\mathcal{E}'$ by x', y', etc. A *μ-measurable functional Hilbert space* is a functional Hilbert space $\mathfrak{F}$ on the basic set $\mathcal{E}$ such that: (a) all the exceptional sets are of measure 0, (b) each $u \in \mathfrak{F}$ is integrable on every $x' \in \mathcal{E}'$, (c) if $\| u \| \neq 0$, *then* $\int_{x'} u \, d\mu \neq 0$ for some $x' \in \mathcal{E}'$, and (d) for every $x' \in \mathcal{E}'$, $\int_{x'} u \, d\mu$ is a continuous linear functional of u.[8]

A μ-measurable functional Hilbert space $\mathfrak{F}$ determines a proper functional Hilbert space $\mathfrak{F}'$ whose basic set is the class $\mathcal{E}'$. $\mathfrak{F}'$ consists of all functions u' to which there corresponds some $u \in \mathfrak{F}$ such that $u'(x') = \int_{x'} u \, d\mu$ for every $x' \in \mathcal{E}'$. The mapping $u \rightarrow u'$ is one to one, and when (u', v') is defined to be (u, v), it becomes a Hilbert space isomorphism between $\mathfrak{F}$ and $\mathfrak{F}'$. The reproducing kernel for $\mathfrak{F}'$ is the function $K'(x', y') = (u_{y'}, u_{x'})$, where $u_{x'} \in \mathfrak{F}$ is such that for every $v \in \mathfrak{F}$, $\int_{x'} v \, d\mu = (v, u_{x'})$.

---

[8] The definition is valid for general incomplete spaces. In case of a complete space, in particular in case of a Hilbert space, (d) follows from (a), (b), (c).

A pseudo-reproducing kernel for a μ-measurable functional Hilbert space $\mathfrak{F}$ is a function $K(x, y)$ with the property that for every x' and y' in $\mathcal{E}'$, $K(x, y)$ is integrable over $x' \times y'$, and $K'(x', y') = \int_{x'} \int_{y'} K(x, y) d\mu(y) d\mu(x)$. It is clear that this condition determines $K(x, y)$ a.e. on $\mathcal{E} \times \mathcal{E}$.[9]

Since $K'(x', y')$ is an additive function of the rectangle $x' \times y'$, it can be extended to an additive set function on the ring generated by the rectangles, so that by the Radon-Nikodym theorem, a necessary and sufficient condition in order that the μ-measurable functional Hilbert space $\mathfrak{F}$ have a pseudo-reproducing kernel is that the function $K'(x', y')$ be an absolutely continuous function of the rectangle $x' \times y'$.

If a measure μ and a function $K(x, y)$ integrable over all $x' \times y'$ are given, then a necessary and sufficient condition in order that $K(x, y)$ be a pseudo-reproducing kernel for some μ-measurable functional Hilbert space $\mathfrak{F}$ is that the function $K'(x', y') = \int_{x'} \int_{y'} K(x, y) \, d\mu(y) \, d\mu(x)$ be a positive matrix on $\mathcal{E}'$. If $K'(x', y')$ is a positive matrix, $\mathfrak{F}$ is constructed as follows. Let $\mathfrak{F}_0$ be the class of all linear combinations $u = \sum \alpha_i u_{y'_i}$, where $u_{y'_i}(x) = \int_{y'_i} K(x, y) \, d\mu(y)$, with the norm

$$(3.1) \qquad \| u \|^2 = \sum \alpha_i \bar{\alpha}_j K'(y'_j, y'_i).$$

It can be proved that $\mathfrak{F}_0$ has a functional completion $\mathfrak{F}$, which is a μ-measurable functional Hilbert space.[10] Obviously, $K(x, y)$ is a pseudo-reproducing kernel for $\mathfrak{F}$.

The proper generalization of Theorem 1 to μ-measurable functional Hilbert spaces and pseudo-reproducing kernels is clear.

---

[9] The beginnings of the theory of measurable spaces and pseudo-reproducing kernels are in the notes [1]. These notions can be defined in an absolute way, independent of a measure given beforehand. The relative notions defined here are sufficient for our needs in the present paper and avoid some of the difficulties inherent in the absolute notions.

[10] The proof is not obvious. It will be given in the development of the general theory of measurable spaces and pseudo-reproducing kernels.

If we put $f = \sum \alpha_i \chi_{y'_i}$, where $\chi_{y'_i}$ is the characteristic function of y'_i, then (3.1) reads

$$(3.2)\quad \textit{If } u = Kf = \int K(x,y)f(y)d\mu(y), \textit{ then } \| u \|^2 = \int Kf(x)\overline{f(x)}d\mu(x).$$

Thus $K(x,y)$ is a pseudo-reproducing kernel if and only if it is the kernel of an integral operator which is positive in the most general sense, i.e., on the class of linear combinations of characteristic functions of measurable sets of finite measure.[11] The corresponding μ-measurable functional Hilbert space is the completion of the range of the integral operator in the norm (3.2). Theorem 1 has the following corollary about positive integral operators.

COROLLARY 1. *If K is a positive integral operator defined on the class of linear combinations of characteristic functions of sets of finite measure, then the kernel of K is non-negative almost everywhere if and only if it is real and for each real u in the range of K there exists $\tilde{u}$ in the completion of the range such that $\tilde{u}(x) \geqq |u(x)|$ almost everywhere and $\| \tilde{u} \| \leqq \| u \|$. The norm in question is that defined in* (3.2).

4. Green's functions. The kernels in which we are chiefly interested are the Green's functions for differential systems. Let A be a linear elliptic self-adjoint differential operator defined in a bounded domain D, and let $\{B_i\}$ be a normal system of boundary operators such that the system $(A; \{B_i\})$ is self-adjoint.[12] The differential system $(A; \{B_i\})$ defines a symmetric operator, which also will be called A, on the Hilbert space L^2 of functions which are square integrable over D. The domain of the operator A is the set of all sufficiently regular functions u on $\bar{D}$ which satisfy the boundary conditions $B_i u = 0$. If the closure of the operator A has a bounded inverse defined everywhere on L^2, and if the inverse is an integral operator, then the kernel $G(x,y)$ of this integral operator is called the Green's function of the system $(A; \{B_i\})$. It is clear that if $u = Gf$, then $\int_D Gf(x)\overline{f(x)}\,dx = \int_D u(x)\overline{Au(x)}\,dx$, so that the quadratic form in (3.2) is non-negative if and only if[13]

$$(4.1)\qquad \| u \|^2 = \int_D Au(x)\overline{u(x)}\,dx,$$

---

[11] We treat the complex case. In the real case it must be assumed that $K(x,y) = K(y,x)$.

[12] We use the terminology introduced in Aronszajn and Milgram [4].

[13] In order to reduce the number of notations we write A instead of the closure of A in some of the formulas.

is non-negative for all u in the domain of A. Since it is assumed that the closure of A has a bounded inverse, if (4.1) is non-negative, there exists a constant $c > 0$ such that

$$\| u \|^2 \geqq c \int_D | u |^2 dx \text{ for } u \text{ in the domain of } A;$$

that is, the differential system $(A; \{B_i\})$ is *positive definite.*

In classical usage the term Green's function is restricted to kernels $G(x, y)$ which are sufficiently regular: if the order of the operator A is $2m$, if its coefficients are sufficiently differentiable, and if the boundary ∂D is sufficiently smooth, then, for fixed $y \in \bar{D}$, $G(x, y)$, as a function of x, should be at least of class C^{2m} in $\bar{D} - \{y\}$. Recent advances in the theory of elliptic partial differential equations have made it possible to prove, in a wide variety of cases, not only the existence of the Green's function as we have defined it, but also the regularity required in the classical definition. The proof, especially the proof of regularity, is based on the property of coerciveness, which has to do with the relation between the quadratic form $\int_D Au\,\bar{u}\,dx$ and the standard m-norm, defined as follows

$$(4.2) \qquad \| u \|_m^2 = \sum_{k=0}^{m} \sum_{k_1 + \cdots + k_n = k} k!(k_1! \cdots k_n!)^{-1} \int_D | \partial^k u / \partial x_1^{k_1} \cdots \partial x_n^{k_n} |^2 \, dx.$$

The quadratic form $\int_D Au\,\bar{u}\,dx$ is said to be *coercive* on the domain of A if there exist constants $c' \geqq 0$ and $N > 0$ such that

$$(4.3) \qquad \int_D Au\bar{u}\,dx + c' \| u \|_0^2 \geqq N \| u \|_m^2 \text{ for all } u \text{ in the domain of } A.$$[14]

If the quadratic form $\int_D Au\,\bar{u}\,dx$ is coercice on the domain of A, the following statement can be proved.

If the coefficients of A and the boundary of D are of class C^{2m}, then the existence of the Green's function $G(x, y)$ in the sense given above is equivalent to the fact that 0 is not an eigenvalue of the closure of A. Furthermore, if $G(x, y)$ exists, the integral operator with kernel $G(x, y)$ is completely continuous in the space L^2.[15]

---

[14] The first coerciveness inequality was proved by Gårding [9] for the case of Dirichlet boundary conditions. The general notion of coerciveness was introduced and investigated by Aronszajn [3]. A more complete presentation of the subject will be given by the same author in a forthcoming paper.

[15] Actually, the above statement is true even when the coefficients and the boundary are only $C^{m-1,1}$; however it is necessary then to consider boundary conditions of order $\geqq m$ in a suitable generalized sense. If we assume the coefficients of A to be of suffi-

If the Green's function of the system $(A;\{B_i\})$ exists and if the system is positive definite, then we see from the last section that the Green's function is a pseudo-reproducing kernel. The corresponding functional Hilbert space is the completion of the domain of A in the norm (4.1). If the norm (4.1) is coercive, it can be proved that the domain of A has a perfect functional completion, the functions of which have derivatives a.e. in the ordinary sense of orders $\leqq m$ in D and of orders $\leqq m-1$ on the boundary of D. This completion contains all functions of class $C^{(m-1,1)}$ (i.e. functions of class C^{m-1} with Lipschitz $(m-1)$-st derivatives) which satisfy the stable boundary conditions, that is those of order $\leqq m-1$. Therefore, Theorem 1 or Corollary 1 give a necessary and sufficient condition in order that the Green's function be non-negative.

It is clear that the foregoing considerations are valid for differential systems considered in a relatively compact subdomain of a differentiable manifold.

5. Green's functions for differential problems of order 2.

We consider a real elliptic linear differential operator A of order 2 on an oriented differentiable manifold M^n of class C^3. Such an operator (or its negative) is expressible in each coordinate patch in the form

$$Au = -\sum a^{ij}\partial^2 u/\partial x^i \partial x^j + \textit{terms of lower order}$$

where a^{ij} is a real symmetric contravariant tensor of rank 2 which forms a positive definite matrix at every point. It is assumed that the tensor a^{ij} is of class C^2, that the coefficients of the first derivatives of u (which do not form a tensor) are of class C^1, and that the coefficient of u is continuous. It is assumed further that the operator A is self-adjoint with respect to some positive density $\rho(x)dx^1\cdots dx^n$ of class C^2.[16]

If $\{a_{ij}\}$ denotes the matrix inverse to $\{a^{ij}\}$ and if a denotes the determinant of $\{a_{ij}\}$, then $g_{ij} = a^{-1/n}\rho^{2/n}a_{ij}$ is a Riemannian metric on M^n. Henceforth M^n is considered as a Riemannian manifold with this metric.[17] If g

---

ciently high Class C^N, it can be proved that $G(x,y)$ exists in the classical sense. A proof of this fact will be published elsewhere. For special types of boundary conditions, including the Dirichlet boundary conditions, a proof of the regularity was given by Nirenberg [10]. A sketchy proof of the statement in the text was given in [11].

[16] This means that $\rho(x)dx^1\cdots dx^n$ is an exterior differential form of rank n, that in each coordinate patch $\rho(x)$ is positive and of class C^2, and that for every pair of functions u and v of class C^2 and 0 outside a compact set,

$$\int Au\bar{v}\rho(x)\,dx^1\cdots dx^n = \int u\overline{Av}\rho(x)\,dx^1\cdots dx^n.$$

[17] We have assumed that the coefficients of A are somewhat more regular than is strictly necessary, in order to be able to use this metric, thereby simplifying a number of the formulas considerably.

denotes the determinant of g_{ij} then $g^{\frac{1}{2}} = \rho$, so A is expressible in any coordinate patch in the form

$$Au = -\sum g^{-\frac{1}{2}}\partial(g^{\frac{1}{2}}a^{ij}\partial u/dx^i)/\partial x^j + \alpha u$$

where α is a continuous real valued function.

Let D be a relatively compact domain in M^n, and let M^{n-1} be a portion of the boundary, ∂D, which is a submanifold of M^n of class C^2. It can be proved that the most general normal system of boundary operators at M^{n-1} which is self-adjoint relative to A is a system composed of a single operator, either the operator $B_0 u = u$ or the operator $B_1 u = \partial u/\partial \nu + bu$, where b is an arbitrary continuous real valued function on M^{n-1}, and where $\partial/d\nu$ is the interior normal derivative in the metric g_{ij}.[18]

It is assumed that the boundary ∂D is a submanifold of M^n of class $C^{(0,1)}$, and that ∂D is also the boundary of $M^n - \bar{D}$. It is assumed in addition that ∂D is piecewise of class C^2 in the following sense: there exist a finite number of disjoint submanifolds M_i^{n-1} of M^n such that $\partial D = \cup \bar{M}_i^{n-1}$; for each i, $\bar{M}_i^{n-1}$ is contained in a submanifold N_i^{n-1} of M^n of class C^2; and in the usual measure on N_i^{n-1}, $\bar{M}_i^{n-1} - M_i^{n-1}$ has measure 0.

Let B be a boundary operator at ∂D obtained by choosing for each M_i^{n-1} either the operator B_0 or one of the operators B_1, (with b continuous on $\bar{M}_i^{n-1}$) and consider the bilinear form

$$(5.1) \quad Q(u,v) = \int_D a^{ij}\partial u/\partial x^i\, \partial\bar{v}/\partial x^j\, g^{\frac{1}{2}}\, dx + \int_D \alpha u\bar{v} g^{\frac{1}{2}}\, dx - \int_{\partial D} p(s) k u\bar{v}\, ds$$

where k is the function on ∂D which on M_i^{n-1} is equal to 0 if the boundary operator chosen on M_i^{n-1} is B_0 and is equal to $-b$ if the boundary operator chosen on M_i^{n-1} is B_1, and where $p(s)$ is the value of the characteristic polynomial of A for the unit normal to ∂D at the point s. If u and v are functions of class C^2 in a neighborhood of $\bar{D}$ and if $Bu = Bv = 0$, then

$$(5.2) \qquad Q(u,v) = \int_D Au\bar{v} g^{\frac{1}{2}}\, dx.$$

The quadratic form $Q(u,u)$ is easily proved to be coercive, even on the class of all functions, a fortiori on the domain of A. Therefore, if the differential system $(A\,;B)$ is positive definite, then the Green's function exists and is a pseudo-reproducing kernel for the completion of the domain of A with the norm $Q(u,u)^{\frac{1}{2}}$. In view of the statements in the last section about this functional space, the scalar product in the complete space is still given by (5.1). Furthermore, the class of Lipschitz functions satisfying the stable boundary conditions (i.e. $B_0 u = 0$ whenever $B = B_0$) forms a dense subspace of the completion. For a function u of this class, $|u|$ is clearly also of this class, and can be taken as the function $\tilde{u}$ in condition (b) of Theorem 1, since $Q(|u|, |u|) = Q(u,u)$. This leads to

---

[18] The terminology used here is that introduced in Aronszajn and Milgram [4]; and all of the calculations used in finding the form of self-adjoint systems are based on the general theory of differential operators on Riemannian manifolds developed there. The operator B_1 has a particularly simple form because of the special choice of the Riemannian metric on M^n.

THEOREM 2. *The three statements below are equivalent.*

(i) *The system $(A;B)$ is positive definite.*

(ii) *The Green's function for the system $(A;B)$ exists and is a pseudo-reproducing kernel.*

(iii) *The Green's function for the system $(A;B)$ exists and is non-negative.*

Proof. The equivalence of statements (i) and (ii) and the fact that they imply statement (iii) are already proved. We assume therefore, that the system $(A;B)$ is not positive definite, but that the Green's function $G(x,y)$ exists, and we show that $G(x,y)$ cannot be non-negative.

According to the part of the theorem which is proved, the Green's function $G_\rho(x,y)$ for the system $(A+\rho;B)$ exists and is non-negative, provided the number $\rho > 0$ is sufficiently large. G_ρ defines a completely continuous integral operator on L^2. Let $1/\mu$ be its largest eigenvalue. By a well-known theorem of Jentsch, $1/\mu$ is positive and there exists a non-negative corresponding eigenfunction f. It is easily verified that $\mu - \rho < 0$ and that $f = (\mu - \rho) Gf$. Obviously, therefore, G cannot be non-negative.

6. Green's functions for differential problems of Order 4. The examples of Duffin and Garabedian mentioned in the introduction show that there is no condition resembling the conditions (i) and (ii) of Theorem 2 which always will ensure that the Green's function of a problem of order 4 is positive. In this section we do not attempt to treat the general question; we only present some interesting special cases.

We assume that M^n is an oriented differentiable manifold of sufficiently high class, that D is a domain in M^n with a sufficiently regular boundary, and that A is a second order differential operator of the type considered in the last section with sufficiently regular coefficients. M^n is given a Riemannian metric as before. We consider differential system of the form $(A^2; B_0, B_2)$ and $(A^2; B_1, B_3)$, where

$$B_0 u = u,$$
$$B_1 u = \partial u/\partial \nu + bu,$$
$$B_2 u = -cp(s)^{-2}\,\partial u/\partial \nu + p(s)^{-1}Au,$$
$$B_3 u = dp(s)^{-2}u + p(s)^{-1}B_1 Au,$$

in which b c, and d are sufficiently regular functions on ∂D. Letting A_0 be the operator on L^2 corresponding to the first system, and A_1 be the operator corresponding to the second, we define

$$Q_0(u,u) = \int_D |Au|^2 g^{\frac{1}{2}}\,dx - \int_{\partial D} c\,|\partial u/\partial \nu|^2\,ds,$$
$$Q_1(u,u) = \int_D |Au|^2 g^{\frac{1}{2}}\,dx - \int_{\partial D} d\,|u|^2\,ds.$$

If u belongs to the domain of A_0, then $\int_D A^2 u\bar{u}\,dx = Q_0(u,u)$ and if u belongs to the domain of A_1, then $\int_D A^2 u\bar{u}\,dx = Q_1(u,u)$. Furthermore, it is not difficult to prove that $Q_0(u,u)$ is coercive on the domain of A_0 and $Q_1(u,u)$ is coercive on the domain of A_1. We get the following

THEOREM 3. *If both systems* $(A;B_0)$ *and* $(A^2;B_0,B_2)$ *are positive definite and if* $c \geqq 0$, *then the Green's function for* $(A^2;B_0,B_2)$ *exists and is non-negative. If both systems* $(A;B_1)$ *and* $(A^2;B_1,B_3)$ *are positive definite and if* $d \geqq 0$, *then the Green's function for* $(A^2;B_1,B_3)$ *exists and is non-negative.*

Proof. Only the first statement will be proved; the second is proved similarly.

The domain of A_0 with the norm $Q_0(u,u)^{\frac{1}{2}}$ has a functional completion whose elements are the functions of the form $u(x) = G_0 f(x)$, where G_0 is the Green's function for the system $(A;B_0)$ and where f is square integrable. Clearly

$$Q_0(u,u) = \int_D |f|^2 g^{\frac{1}{2}}\,dx - \int_{\partial D} c\,|\partial u/\partial \nu|^2\,ds.$$

Since $G_0 \geqq 0$, $\partial G_0/\partial \nu \geqq 0$. Hence the function $\tilde{u}(x) = G_0\,|f|(x)$ has the properties $\tilde{u}(x) \geqq |u(x)|$ and $\partial \tilde{u}/\partial \nu \geqq |\partial u/\partial \nu|$. Since also $c \geqq 0$ it follows that $Q_0(\tilde{u},\tilde{u}) \leqq Q_0(u,u)$.

Remark. If $(A;B_0)$ is positive definite, then, for sufficiently small c, $(A^2;B_0,B_2)$ is also positive definite. If $c = 0$, the statement of the last theorem is trivial, since Green's function for the system $(A^2;B_0,1/p(s)A)$ is

$\int_D G_0(x,z)\,G_0(z,y)\,g^{\frac{1}{2}}\,dz$. A similar remark holds for the system $(A^2; B_1, B_3)$ and the function d.

UNIVERSITY OF KANSAS.

REFERENCES.

[1] N. Aronszajn, " Les noyaux pseudo-reproduisants. Noyaux pseudo-reproduisants et complétion des classes hilbertiennes." " Complétion fonctionnelle de certaines classes hilbertiennes." " Propriétés de certaines classes hilbertiennes completées," *Comptes Rendus*, vol. 226 (1948), pp. 456, 537, 617, 700.

[2] ———, " Theory of reproducing kernels," *Transactions of the American Mathematical Society*, vol. 68 (1950), pp. 337-404.

[3] ———, *On coercive integro-differential quadratic forms*, Conference on Partial Differential Equations, University of Kansas, Summer, 1954.

[4] N. Aronszajn and A. N. Milgram, " Differential operators on Riemannian manifolds," *Rendiconti del Circolo Matematico di Palermo*, ser. 2, vol. 2 (1953), pp. 1-61.

[5] N. Aronszajn and K. T. Smith, " Functional spaces and functional completion," *Annales de l'Inst. Fourier de Grenoble*, vol. 6 (1955-56), pp. 125-185.

[6] S. Bergman and M. Schiffer, " Kernel functions in the theory of partial differential equations of elliptic type," *Duke Mathematical Journal*, vol. 15 (1948), pp. 535-566.

[7] R. J. Duffin, " On a question of Hadamard concerning superbiharmonic functions," *Journal of Mathematics and Physics*, vol. 27 (1949), pp. 253-258.

[8] P. R. Garabedian, "A partial differential equation arising in conformal mapping," *Pacific Journal of Mathematics*, vol. 1 (1951), pp. 485-524.

[9] L. Gårding, " Le problème de Dirichlet pour les équations aux derivées partielles élliptiques dans des domaines bornés," *Comptes Rendus*, Paris, vol. 233 (1951), pp. 1554-1556.

[10] L. Nirenberg, " Remarks on strongly elliptic partial differential equations," *Communications on Pure and Applied Mathematics*, vol. 8 (1955), pp. 649-675.

[11] K. T. Smith, *Functional spaces, functional completion, and differential problems*, Conference on Partial Differential Equations, University of Kansas, Summer, 1954.

[12] E. Hopf, " Elementare Bemerkungen über die Lösungen partieller Differentialgleichungen zweiter Ordnung vom elliptischen Typus," *Sitzungsberichte der Preussischen Akademie der Wissenschaften*, vol. 1927, pp. 147-152.

[13] K. Bleuler, " *Ueber den Rolle'schen Satz für den Operator* $\Delta u + \lambda u$ *und die damit zusammenhängenden Eigenschaften der Green'schen Funktion*," Zürich (Dissertation), 1941-1942.

GROUPS WHICH ACT ON S^n WITHOUT FIXED POINTS.*

By JOHN MILNOR.[1]

We will study the question of which finite groups can act on an n-sphere without fixed points. The main result (Section 1) is that any element of order two in such a group must lie in the center. A general survey of the problem is given in Section 2. The special case $n = 3$ is considered in Section 3.

An equivalent formulation of the problem is the following. Which groups can occur as the fundamental groups of manifolds M^n for which the universal covering space $\tilde{M}^n$ is homeomorphic to S^n. More generally one might only require that $\tilde{M}^n$ have the homotopy type of S^n. For example, any 3-manifold with a finite fundamental group satisfies this more general condition. (Such manifolds are classified up to homotopy type by the fundamental group together with the k-invariant (see Olum [3] Theorem IV.))

The author is indebted to helpful discussions with A. Shapiro.

1. Elements of order 2.

A known theorem asserts that, for every map $f\colon S^n \to S^n$ of odd degree, there exists a pair of antipodal points whose images under f are also antipodal. (*Proof.* Let T denote the antipodal map, and suppose that $f(x)$, $f(Tx)$ are never antipodal. Let $g(x)$ denote the midpoint of the shortest great circle arc joining $f(x)$ to $f(Tx)$. Since $g(x) = g(Tx)$, the map $g\colon S^n \to S^n$ can be factored through n-dimensional projective space, and therefore has even degree. But since g is homotopic to f, this contradicts the assumption that f has odd degree.)

We will need the following generalization, which will be proved by a similar method.

THEOREM 1. *Let M^n be a manifold having the mod two homology of the n-sphere, and let $T\colon M^n \to M^n$ be a map of period two without fixed points. Then for every map $f\colon M^n \to M^n$ of odd degree there exists a point $x \in M^n$ such that $Tf(x) = fT(x)$.*

---

* Received April 2, 1957.

[1] The author holds an Alfred P. Sloan fellowship.

As an immediate consequence we have:

Corollary 1. *Suppose that the group G acts without fixed points on a manifold M^n having the mod two homology of the n-sphere. Then any element of order two in G belongs to the center.*

Proof. Let $T \in G$ have order two, and let U be any other element of G. Then Theorem 1 implies that we can find a point $x \in M^n$ with $TU(x) = UT(x)$. Since G acts without fixed points, this implies that $TU = UT$, which proves the corollary.

As an example we have

Corollary 2. *The symmetric group on three elements cannot operate on the n-sphere without fixed points.*

Remark. It is known that the group $Z_2 + Z_2$ cannot operate on S^n without fixed points. (See Section 2.) Therefore Corollary 1 implies that the group G can have at most one element of order 2. Conversely if G has only one element of order 2, then this element clearly belongs to the center.

Proof of Theorem 1. Let A denote the set of all points (x, Tx) in $M^n \times M^n$. Let $M^n * M^n$ denote the symmetric product, and let A' denote the set of points $\{x, Tx\}$ in $M^n * M^n$. If $f\colon M^n \to M^n$ satisfies $Tf(x) \neq fTx$ for all x, then there is a commutative diagram

$$\begin{tikzcd}
 & M_n \\
M^n \arrow[ur, "f"] \arrow[r, "f_1"] \arrow[d, "i_1"] & M^n \times M^n - A \arrow[u, "p_1"'] \arrow[d, "i_2"] \\
M^n/T \arrow[r, "f_2"] & M^n * M^n - A'
\end{tikzcd}$$

where i_1 and i_2 are the natural identification maps, and where

$$f_1(x) = (f(x), f(Tx)), \qquad f_2\{x, Tx\} = \{f(x), f(Tx)\}, \qquad p_1(x, y) = x.$$

Thus we are almost able to factor f through the "projective space" M^n/T, except that the map i_2 goes in the wrong direction.

LEMMA 1. *The homomorphism*

$$i_{2*}: H_k(M^n \times M^n - A) \to H_k(M^n * M^n - A')$$

is an isomorphism for all dimensions k.

(Singular homology with the coefficient group Z_2 is to be understood.)

Proof. It will first be shown that the projection $p_1: M^n \times M^n - A \to M^n$ is a locally trivial fibre map with fibre $p_1^{-1}(x) \approx M^n - Tx$. Given any closed n-cell $\bar{C}$ in M^n with interior C, choose a homeomorphism g of $T\bar{C}$ onto the unit ball $\bar{B}$ in euclidean n-space. Define the map $\lambda: B \times \bar{B} \to \bar{B}$ by

$$\lambda(\vec{v}, \vec{w}) = \vec{w} + (1 - \| \vec{w} \|)\vec{v},$$

where B denotes the interior of $\bar{B}$. Note that for each fixed vector $\vec{v} \in B$ the correspondence $\vec{w} \to \lambda(\vec{v}, \vec{w})$ defines a homeomorphism of $\bar{B}$ onto itself leaving the boundary fixed and carrying the center $\vec{0}$ into $\vec{v}$. The required local product structure

$$\phi: C \times (M^n - g^{-1}(\vec{0})) \to p_1^{-1}(C)$$

is now defined by

$$\phi(x, y) = (x, y) \text{ if } y \notin TC, \quad \phi(x, y) = (x, g^{-1}\lambda(gTx, gy)) \text{ if } y \in T\bar{C}.$$

It is not hard to show that ϕ is a homeomorphism.

Thus p_1 is a fibre map. According to the Lefschetz duality theorem, the fibre $M^n - Tx$ has the homology of a point. Therefore the induced homomorophism

$$p_{1*}: H_*(M^n \times M^n - A) \to H_*(M^n)$$

is an isomorphism. Let Δ denote the diagonal in $M^n \times M^n - A$ and let Δ' denote its image in $M^n * M^n - A'$. Since the diagonal map $M^n \to \Delta \subset M^n \times M^n - A$ is a cross-section of the fibre map p_1, it follows that the group $H_*(M^n \times M^n - A \bmod \Delta)$ is zero.

Next we will show that the "relative" 2-fold covering map

$$(M^n \times M^n - A, \Delta) \xrightarrow{c} (M^n * M^n - A', \Delta')$$

has a Gysin cohomology sequence. The difficulty lies in the fact that this map is a covering only in the complement of the diagonal Δ. If U denotes any symmetric neighborhood of Δ, and U' denotes its image in the collapsed space, consider the diagram

$$\begin{tikzcd}
(M^n \times M^n - A - \Delta, U - \Delta) \arrow[r, "e"] \arrow[d, "c_1"] & (M^n \times M^n - A, U) \arrow[d, "c_2"] & (M^n \times M^n - A, \Delta) \arrow[l] \arrow[d, "c"] \\
(M^n * M^n - A' - \Delta', U' - \Delta') \arrow[r, "e'"] & (M^n * M^n - A', U') & (M^n * M^n - A', \Delta'). \arrow[l]
\end{tikzcd}$$

Since c_1 is a true 2-fold covering, it has a Gysin sequence. Since e and e' are excisions, the map c_2 also has a Gysin sequence. But since Δ and $M^n \times M^n - A$ are both absolute neighborhood retracts, the cohomology group $H^*(M^n \times M^n - A \bmod \Delta)$ is the direct limit of the groups $H^*(M^n \times M^n - A \bmod U)$ as U ranges over all symmetric neighborhoods. A similar description holds for $H^*(M^n * M^n - A' \bmod \Delta')$. Since the direct limit of exact sequences is again an exact sequence, this gives us the required Gysin sequence

$$\begin{aligned}
&\to H^k(M^n \times M^n - A, \Delta) \to H^k(M^n * M^n - A', \Delta') \\
&\qquad \to H^{k+1}(M^n * M^n - A', \Delta') \xrightarrow{c^*} H^{k+1}(M^n \times M^n - A, \Delta) \to .
\end{aligned}$$

Since the left and right hand groups in this sequence are known to be zero, induction shows that the middle groups are also zero. Therefore the corresponding homology groups $H_k(M^n * M^n - A' \bmod \Delta')$ are zero. This implies that the inclusion homomorphism $H_*(\Delta') \to H_*(M^n * M^n - A')$ is an isomorphism. It has already been shown that the inclusion homomorphism $H_*(\Delta) \to H_*(M^n \times M^n - A)$ is an isomorphism. Since the map $i_2 | \Delta \colon \Delta \to \Delta'$ is a homeomorphism, this implies that

$$i_{2*} \colon H_*(M^n \times M^n - A) \to H_*(M^n * M^n - A')$$

is an isomorphism; which completes the proof of Lemma 1.

Consider the diagram

$$\begin{tikzcd}
 & H_n(M^n) \\
H_n(M^n) \arrow[ur, "f_*"] \arrow[r, "f_{1*}"] \arrow[d, "i_{1*}"] & H_n(M^n \times M^n - A) \arrow[u, "p_{1*}"'] \arrow[d, "i_{2*}"'] \\
H_n(M^n/T) \arrow[r, "f_{2*}"] & H_n(M^n * M^n - A').
\end{tikzcd}$$

It is clear that $i_{1*} = 0$. Since i_{2*} is an isomorphism, this implies that $f_{1*} = 0$, and hence $f_* = 0$. This contradicts the hypothesis of Theorem 1, and completes the proof.

2. A survey of the problem.

We will say that a group G has *property I* if every abelian subgroup is cyclic. This is equivalent to the condition that every p-subgroup is either cyclic or, for $p = 2$, a generalized quaternion group.[2]

According to P. Smith [5], every group which acts on a homology sphere without fixed points has property I. This result can be given more precision by noting that if G acts on S^n without fixed points then[2] the cohomology ring $H^*(G, Z)$ has period $n + 1$. According to Artin and Tate a group has property I if and only if it has periodic cohomology.[2]

An enumeration of all groups having property I has been given by Zassenhaus ([8] Theorem 7) in the solvable case, and by M. Suzuki ([6] Theorem E) in the non-solvable case.

Corollary 1 gives a further restriction which the group G must satisfy. (For example the non-abelian group of order $2p$ has property I and yet cannot act on a sphere without fixed points.) However it seems likely that more restrictions are still needed.

If G is required to act orthogonally on S^n, then the problem has been solved by Zassenhaus. ([8] Theorems 3, 8, 11, 16. See also Vincent [7].) At present, every group which is known to act on S^n without fixed points can actually act orthogonally.

The following two results of Zassenhaus are especially striking. We will say that G has *property II* if every subgroup of order pq is cyclic. Here p and q range over not necessarily distinct primes.

(a) Every group which acts orthogonally on S^n without fixed points has property II.

(b) Every solvable group with property II can act orthogonally on some S^n without fixed points.

Evidently the major unsolved problem is the following. Does every group which acts on S^n without fixed points have property II? Smith's result implies that every subgroup of order p^2 is cyclic, and Corollary 1 implies that every subgroup of order $2p$ is cyclic. The first unsolved case is therefore the following. Can the non-abelian group of order 21 act on a sphere without fixed points?

---

[2] See Cartan and Eilenberg [1], Chapters XII, Section 11 and XVI, Section 9.

3. The case $n = 3$.

The main object of this section will be to summarize the gap in our knowledge concerning groups which act on the 3-sphere without fixed points (or concerning finite fundamental groups of closed 3-manifolds). This will be done by enumerating those groups which satisfy the known restrictions, but which cannot act orthogonally on S^3 without fixed points. (Theorem 3.) It is interesting to note that the groups in question are all solvable, and are all known to act on higher dimensional spheres without fixed points. The proofs are routine, and will be largely omitted.

The sphere S^3 is itself a topological group, isomorphic to the two-fold covering space of the rotation group $SO(3)$. Let $h\colon S^3 \to SO(3)$ denote the covering. Then each finite subgroup G of $SO(3)$ determines a subgroup $h^{-1}(G)$ of S^3 with twice as many elements. Corresponding to the dihedral group with $2n$ elements, $n \geqq 2$, we obtain a subgroup Q_{4n} of S^3 with presentation $(x, y\colon x^2 = (xy)^2 = y^n)$. (If n is a power of 2, then Q_{4n} is the generalized quaternion group.) Corresponding to the tetrahedral, octahedral, and icosohedral groups, we obtain subgroups P_{24}, P_{48} and P_{120} of S^3 with presentations $(x, y\colon x^2 = (xy)^3 = y^n, x^4 = 1)$, where $n = 3, 4, 5$ respectively.

The next theorem is essentially due to Hopf [2]. For a detailed study of the quotient manifolds see Seifert and Threlfall [4].

THEOREM 2. *The following is a list of all finite groups which act orthogonally on S^3 without fixed points.*

1) *The groups* 1, Q_{8n}, P_{48}, *and* P_{120}.

2) *The groups* $D_{2^k(2n+1)}$ *with presentation*

$$(x, y\colon x^{2^k} = 1,\ y^{2n+1} = 1,\ xyx^{-1} = y^{-1}) \quad \textit{where } k \geqq 2, n \geqq 1.$$

3) *The groups* $P'_{8\cdot 3^k}$ *with presentation*

$$(x, y, z\colon x^2 = (xy)^2 = y^2, zxz^{-1} = y, zyz^{-1} = xy, z^{3^k} = 1) \quad \textit{where } k \geqq 1.$$

4) *The direct product of any of these groups with a cyclic group of relatively prime order.*

(Note that the groups Q_{4n} with n odd are isomorphic to D_{4n}. The group P_{24} is isomorphic to P'_{24}.)

For a sketch of the proof we refer to Hopf's paper.

Given relatively prime positive integers $8n$, k, l let $Q(8n, k, l)$ denote the group with presentation

$$(x, y, z\colon x^2 = (xy)^2 = y^{2n}, z^{kl} = 1, xzx^{-1} = z^r, yzy^{-1} = z^{-1}),$$

where $r \equiv -1 \pmod{k}$, $r \equiv +1 \pmod{l}$. Thus for $k = l = 1$ we have the group Q_{8n}. Note that $Q(8n, k, l)$ is isomorphic to $Q(8n, 1, k)$. For n odd, the three integers n, k, l may be permuted without changing the group.

For any odd integer r let P''_{48r} denote the group extension with subgroup Z_r and factor group P_{48} such that the 3-Sylow subgroup is cyclic, and such that P_{48} acts on Z_r as follows. Elements in the commutator subgroup P_{24} act trivially, while the remaining elements of P_{48} carry each element of Z_r into its inverse.

THEOREM 3. *The following is a list of all finite groups which* (a) *have cohomology of period* 4, (b) *have at most one element of order* 2, *and* (c) *are not listed in Theorem* 2.

1) *The groups $Q(8n, k, l)$ with $8n, k, l$ pairwise relatively prime and either* a) *n odd and $n > k > l \geqq 1$ or* b) *n even and $n \geqq 2$, $k > l \geqq 1$.*

2) *The groups P''_{48r} with r odd, $r \geqq 3$.*

3) *The product of any of these groups with a cyclic group of relativcly prime order.*

Thus the smallest group which may or may not be the fundamental group of a 3-manifold is $Q(16, 3, 1)$ with 48 elements.

A few of these groups can be eliminated by a different argument:

LEMMA 2. *If r is not a power of 3, then P''_{48r} cannot be the fundamental group of a 3-manifold.*

Proof. Let $r = 3^{k-1}s$ with $(s, 6) = 1$, $s \geqq 5$. Then P''_{48r} contains a normal subgroup isomorphic to $P'_{8 \cdot 3^k}$, the factor group being isomorphic to D_{2s}.

Now given a manifold M^3 with $\pi_1(M^3) \approx P''_{48r}$ let $M_1{}^3$ denote the $2s$-fold covering with fundamental group $\pi_1(M_1{}^3) = P'_{8 \cdot 3^k}$. The first homology group of $M_1{}^3$ is the abelianized group, which turns out to be Z_3. Therefore $M_1{}^3$ has the mod two homology of the 3-sphere. But the group D_{2s} of covering transformations acts on $M_1{}^3$ without fixed points. Since D_{2s} has an element of order two which is not in the center, this contradicts Corollary 1, and completes the proof.

The proof of Theorem 3 consists in going over the groups listed by Zassenhaus and Suzuki, eliminating those which do not have cohomology of period four. The spectral sequence of a group extension is the main tool needed.

PRINCETON UNIVERSITY.

REFERENCES.

[1] H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton, 1956.

[2] H. Hopf, "Zum Clifford-Kleinschen Raumproblem," *Mathematische Annalen*, vol. 95 (1925-26), pp. 313-319.

[3] P. Olum, "Mappings of manifolds and the notion of degree," *Annals of Mathematics*, vol. 58 (1953), pp. 458-480.

[4] H. Seifert and W. Threlfall, "Topologische Untersuchung der Diskontinuitätsbereiche endlicher Bewegungsgruppen des dreidimensionalen sphärischen Raumes," *Mathematische Annalen*, vol. 104 (1930-31), pp. 1-70.

[5] P. Smith, "Permutable periodic transformations," *Proceedings of the National Academy of Sciences*, vol. 30 (1944), pp. 105-108.

[6] M. Suzuki, "On finite groups with cyclic Sylow subgroups for all odd primes," *American Journal of Mathematics*, vol. 77 (1955), pp. 657-691.

[7] G. Vincent, "Les groupes linéaires finis san points fixes," *Commentarii Mathematici Helvetici*, vol. 20 (1947), pp. 117-171.

[8] H. Zassenhaus, "Über endliche Fastkörper," *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, vol. 11 (1936), pp. 187-220.

ON A CLASS OF TRANSFORMATION GROUPS.*

By Andrew M. Gleason and Richard S. Palais.

In order to apply our rather deep understanding of the structure of Lie groups to the study of transformation groups it is natural to try to single out a class of transformation groups which are in some sense naturally Lie groups. In this paper we introduce such a class and commence their study.

In Section 1 the notion of a Lie transformation group is introduced. Roughly, these are groups H of homeomorphisms of a space X which admit a Lie group topology which is strong enough to make the evaluation mapping $(h, x) \rightarrow h(x)$ of $H \times X$ into X continuous, yet weak enough so that H gets all the one-parameter subgroups it deserves by virtue of the way it acts on X (see the definition of admissibly weak below). Such a topology is uniquely determined if it exists and our efforts are in the main concerned with the question of when it exists and how one may effectively put one's hands on it when it does. A natural candidate for this so-called Lie topology is of course the compact-open topology for H. However, if one considers the example of a dense one-parameter subgroup H of the torus X acting on X by translation, it appears that this is not the general answer. In this example if we modify the compact-open topology by adding to the open sets all their arc components (getting in this way what we call the modified compact-open topology), we get the Lie topology of H. That this is a fairly general fact is one of our main results (Theorem 5.14). The latter theorem moreover shows that the reason that the compact-open topology was not good enough in the above example is connected with the fact that H was not closed in the group of all homeomorphisms of X, relative to the compact-open topology. Theorem 5.14 also states that for a large class of interesting cases the weakness condition for a Lie topology is redundant.

The remainder of the paper is concerned with developing a certain criterion for deciding when a topological group is a Lie group and applying this criterion to derive a general necessary and sufficient condition for groups of homeomorphisms of locally compact, locally connected finite dimensional metric spaces to be Lie transformation groups. The criterion is remarkable in that local compactness is not one of the assumptions. It states in fact

---

* Received February 11, 1957.

that a locally arcwise connected topological group is a Lie group provided that its compact metrizable subspaces are of bounded dimension.

1. Lie transformation groups. Let G be a topological group and X a topological space. By an *action* of G on X we mean a homomorphism $\phi\colon g \to \phi_g$ of G into the group of homeomorphisms of X such that the map $(g, x) \to \phi_g(x)$ of $G \times X$ into X is continuous. If H is a group of homeomorphisms of X, then a topology for H will be called *admissibly strong* if it renders the map $(h, x) \to h(x)$ of $H \times X \to X$ continuous. We note that we do *not* demand of an admissibly strong topology that it make H a topological group; however if H is a topological group in a given topology, then clearly that topology is admissibly strong if and only if it makes the identity map of H on itself an action of H on X. Moreover if we denote by R the additive group of real numbers then:

1. 1. PROPOSITION. *Let H be a topological group whose underlying group is a group of homeomorphisms of a space X. If the topology of H is admissibly strong, then each one-parameter subgroup of H is an action of R on X.*

We shall call a topology for a group H of homeomorphisms of a space X *admissibly weak* if every action of R on X whose range is in H is a continuous map of R into H with respect to this topology. Again we note that an admissibly weak topology for H is not required to make H a topological group. However from 1.1 and the definition of admissibly weak we clearly have:

1. 2. PROPOSITION. *Let H be a topological group whose underlying group is a group of homeomorphisms of a space X. If the topology for H is both admissibly weak and admissibly strong then the one-parameter subgroups of H are exactly the actions of R on X whose ranges lie in H.*

The terminology 'admissibly strong' and 'admissibly weak' is justified by the following trivial observation.

1. 3. PROPOSITION. *Let H be a group of homeomorphisms of a space X. A topology for H which is stronger (weaker) than an admissibly strong (weak) topology is itself admissibly strong (weak).*

Some authors use the term admissible for topologies that we call admissibly strong. For this reason we shall not succumb to the temptation of calling admissible those topologies which are at once admissibly strong and admissibly weak.

1.4. *Definition.* Let H be a group of homeomorphisms of a space X. A *Lie topology* for H is a topology for H which is both admissiblly strong and admissibly weak and which furthermore makes H a Lie group.

The following well-known fact is an immediate consequence of the existence of canonical coordinate systems of the second kind in Lie groups.

1.5. LEMMA. *Let G and H be Lie groups and h a homomorphism of the underlying group of G into the underlying group of H. A necessary and sufficient condition for h to be continuous is that $h \circ \phi$ be a one parameter subgroup of H whenever ϕ is a one-parameter subgroup of G. In particular, if G and H have the same underlying group and the same one-parameter subgroups, they are identical.*

The following proposition follows directly from 1, 2, 1.5, and the definition of a Lie topology.

1.6. PROPOSITION. *A group of homeomorphisms of a topological space admits at most one Lie topology.*

1.7. *Definition.* A group of homeomorphisms of a topological space X will be called a *Lie transformation group of X* if it admits a Lie topology.

The unique Lie topology for a Lie transformation group G will be called the Lie topology for G and properties meaningful for a Lie group when used in reference to G are to be interpreted relative to its Lie topology.

2. A theorem on arcwise connected spaces. A theorem somewhat more general than the next lemma is proved on page 115 of [6], and a still more general result is indicated in exercise 7, page 80 of [8].

2.1. LEMMA. *A partitioning of the unit interval into at most countably many disjoint closed sets is trivial, i. e., contains only one element.*

2.2. THEOREM. *A partitioning of an arcwise connected space X into at most countably many disjoint closed sets is trivial.*

Proof. Let $\{E_n\}$ be such a partitioning and let $p, q \in X$. We must show that p and q are in the same E_n. Let f be a continuous map of the unit interval into X such that $f(0) = p$ and $f(1) = q$. Applying the lemma to the partitioning $\{f^{-1}(E_n)\}$ of the unit interval we see that for some n $f^{-1}(E_n)$ is the entire unit interval. Hence $p = f(0)$ and $q = f(1)$ belong to E_n.

3. Making a topology locally arcwise connected. Most, if not all, of the results of this section are known, but they belong to the realm of folk-theorems and are apparently not easily available in the literature.

Let $(X, \mathcal{T})$ be a topological space (i. e., X a set and $\mathcal{T}$ a topology for X) and let $\mathcal{B}$ be the set of arc components of all open subspaces of $(X, \mathcal{T})$. Suppose B_1 and B_2 are elements of $\mathcal{B}$ and let B_i be an arc component of $\mathcal{O}_i \in \mathcal{T}$. Then if $p \in B_1 \cap B_2$, the arc component of p in $\mathcal{O}_1 \cap \mathcal{O}_2$, which belongs to $\mathcal{B}$, is clearly a subset of $B_1 \cap B_2$. Thus $B_1 \cap B_2$ is a union of sets from $\mathcal{B}$ and hence $\mathcal{B}$ is a base for a new topology $\mathcal{M}(\mathcal{T})$ for X which is clearly stronger than $\mathcal{T}$.

3.1. *Definition.* We define an operation $\mathcal{M}$ on topologies as follows: if $\mathcal{T}$ is a topology for a set X then $\mathcal{M}(\mathcal{T})$ is the topology for X which has as a base all arc components of open subspaces of $(X, \mathcal{T})$.

The following theorem summarizes some of the most important properties of the operation $\mathcal{M}$.

3.2. THEOREM. *Let $(X, \mathcal{T})$ be a topological space.*

(1) *If $\mathcal{T}$ satisfies the first axiom of countability, so does $\mathcal{M}(\mathcal{T})$.*

(2) *If Z is a locally arcwise connected space and f is a function from Z into X continuous relative to the topology $\mathcal{T}$, then f is also continuous relative to $\mathcal{M}(\mathcal{T})$. In particular $(X, \mathcal{T})$ and $(X, \mathcal{M}(\mathcal{T}))$ have the same arcs.*

(3) *$(X, \mathcal{M}(\mathcal{T}))$ is locally arcwise connected, and in fact $\mathcal{M}(\mathcal{T})$ can be characterized as the weakest locally arcwise connected topology for X which is stronger than $\mathcal{T}$. Hence $\mathcal{M}$ is idempotent.*

(4) *The components of an open subset of $(X, \mathcal{M}(\mathcal{T}))$ are just its arc components when regarded as a subspace of $(X, \mathcal{T})$. In particular the components of $(X, \mathcal{M}(\mathcal{T}))$ are the arc components of $(X, \mathcal{T})$.*

(5) *If X is a group and $(X, \mathcal{T})$ a topological group, then $(X, \mathcal{M}(\mathcal{T}))$ is also a topological group and it has the same one-parameter subgroups as $(X, \mathcal{T})$.*

Proof. Given $x \in X$ and a countable base $\{\mathcal{O}_n\}$ for the $\mathcal{T}$-neighborhoods of x we get a countable base $\{\mathcal{O}_n'\}$ for the $\mathcal{M}(\mathcal{T})$-neighborhoods of x by taking $\mathcal{O}_n'$ to be the arc component of x in $\mathcal{O}_n$ (relative to the topology $\mathcal{T}$, of course). This proves (1).

Let $\mathcal{B}$ be the set of all arc components of open subspaces of $(X, \mathcal{T})$ so that by definition $\mathcal{B}$ is a base for $\mathcal{M}(\mathcal{T})$.

Suppose f is a function from the locally arcwise connected space Z into X which is continuous relative to $\mathcal{T}$. Given $B \in \mathcal{B}$ we will show that $f^{-1}(B)$ is open in Z which will prove (2). By definition of $\mathcal{B}$ we can choose $\mathcal{O} \in \mathcal{T}$ such that B is an arc component of $\mathcal{O}$. Given $p \in f^{-1}(B)$ let W be the arc component of p in $f^{-1}(\mathcal{O})$. Then $f(W)$ is arcwise connected, included in $\mathcal{O}$, and meets B at $f(p)$; hence $f(W) \subseteq B$. Since Z is locally arcwise connected and $f^{-1}(\mathcal{O})$ is open, W is open. Thus a neighborhood of p is included in $f^{-1}(B)$ so $f^{-1}(B)$ is open.

Next let $B \in \mathcal{B}$. By definition of $\mathcal{B}$, B is arcwise connected when regarded as a subspace of $(X, \mathcal{T})$. Hence by (2) B is an arcwise connected subspace of $(X, \mathcal{M}(\mathcal{T}))$. Thus $\mathcal{M}(\mathcal{T})$ has a base consisting of arcwise connected sets so, by definition, $\mathcal{M}(\mathcal{T})$ is locally arcwise connected. Since every $\mathcal{O} \in \mathcal{T}$ is the union of its arc components and hence belongs to $\mathcal{M}(\mathcal{T})$ it follows that $\mathcal{M}(\mathcal{T})$ is stronger than $\mathcal{T}$. Suppose $\mathcal{T}'$ is a locally arcwise topology for X stronger than $\mathcal{T}$. Then the identity mapping f of $Z = (X, \mathcal{T}')$ into $(X, \mathcal{T})$ is continuous and hence, by (2), f is a continuous map of Z into $(X, \mathcal{M}(\mathcal{T}))$, i.e., $\mathcal{T}'$ is stronger that $\mathcal{M}(\mathcal{T})$. This proves (3).

If $\mathcal{O}$ is an open subspace of $(X, \mathcal{M}(\mathcal{T}))$ then, since $\mathcal{M}(\mathcal{T})$ is locally arcwise connected, the components of $\mathcal{O}$ are the same as the arc components of $\mathcal{O}$. On the other hand, by (2), the arc components of $\mathcal{O}$ are the same whether $\mathcal{O}$ is regarded as a subspace of $(X, \mathcal{T})$ or $(X, \mathcal{M}(\mathcal{T}))$. This proves (4).

Finally, suppose that X is a group and let f be the map $(x, y) \rightarrow xy^{-1}$ of $X \times X \rightarrow X$. If $(X, \mathcal{T})$ is a topological group then f is a continuous map of $(X, \mathcal{T}) \times (X, \mathcal{T}) \rightarrow (X, \mathcal{T})$ and *a fortiori* (since $\mathcal{M}(\mathcal{T})$ is stronger than $\mathcal{T}$) f is a continuous map of $(X, \mathcal{M}(\mathcal{T})) \times (X, \mathcal{M}(\mathcal{T})) \rightarrow (X, \mathcal{T})$. Since by (3) $(X, \mathcal{M}(\mathcal{T})) \times (X, \mathcal{M}(\mathcal{T}))$ is locally arcwise connected, it follows from (2) that f is a continuous map of

$$(X, \mathcal{M}(\mathcal{T})) \times (X, \mathcal{M}(\mathcal{T})) \rightarrow (X, \mathcal{M}(\mathcal{T})),$$

i.e., that $(X, \mathcal{M}(\mathcal{T}))$ is a topological group. It also follows from (2) that $(X, \mathcal{T})$ and $(X, \mathcal{M}(\mathcal{T}))$ have the same arcs and hence the same one-parameter subgroups. This proves (5).

3.3. *Definition.* If $\mathfrak{G} = (G, \mathcal{T})$ is a topological group, then we call $(G, \mathcal{M}(\mathcal{T}))$ the *associated locally arcwise connected group of* $\mathfrak{G}$.

4. Weakening the topology of a Lie group.

4. 1. THEOREM. *Let ϕ be a one-to-one representation of a locally compact group G satisfying the second axiom of countability onto a locally arcwise connected group H. Then ϕ^{-1} is continuous, i. e., ϕ is an isomorphism of G with H.*

Proof. Let V be a compact neighborhood of e_G, the identity of G. It will suffice to show that $\phi(V)$ is a neighborhood of e_H, the identity of H. Choose an open, symmetric neighborhood U of e_G such that $\bar{U}^2 \subseteq V$. Then $V - U$ is compact, so $\phi(V - U)$ is compact and hence that complement of $\phi(V - U)$ is a neighborhood of e_H. Let X be an arcwise connected neighborhood of e_H such that XX^{-1} does not meet $\phi(V - U)$.

Given g_1 and g_2 in $\phi^{-1}(X)$ we put $g_1 \sim g_2$ if and only in $g_1 g_2^{-1} \in \bar{U}$. Since $\bar{U}$ is a symmetric neighborhood of e_G, it follows that $\sim$ is a symmetric, reflexive relation on $\phi^{-1}(X)$. If $g_1 \sim g_2$ and $g_2 \sim g_3$ then $g_1 g_3^{-1} = (g_1 g_2^{-1})(g_2 g_3^{-1}) \in \bar{U}^2 \subseteq V$. But $\phi(g_1 g_3^{-1}) = \phi(g_1)\phi(g_3)^{-1} \in XX^{-1}$ and since XX^{-1} is disjoint from $\phi(V - U)$, it follows that $g_1 g_3^{-1} \in U \subseteq \bar{U}$ so $g_1 \sim g_3$. Hence $\sim$ is also transitive and hence is an equivalence relation on $\phi^{-1}(X)$. Let $\{g_\alpha\}$ be a complete set of representatives of $\phi^{-1}(X)$ under $\sim$, one of which we can take to be e_G. Given $g \in \phi^{-1}(X)$ we can find a g_α such that $g_\alpha \sim g$ so $g \in \bar{U} g_\alpha$. Thus $\{\bar{U} g_\alpha\}$ is a covering of $\phi^{-1}(X)$. If $g \in \bar{U} g_\alpha \cap \bar{U} g_\beta$, then $g_\alpha g^{-1} \in \bar{U}^{-1} = \bar{U}$ and $g g_\beta^{-1} \in \bar{U}$, so $g_\alpha g_\beta^{-1} \in \bar{U}^2 \subseteq V$. But $\phi(g_\alpha g_\beta^{-1}) \in XX^{-1}$ which is disjoint from $\phi(V - U)$ so $g_\alpha g_\beta^{-1} \in U \subseteq \bar{U}$ so $g_\alpha \sim g_\beta$ and $\alpha = \beta$. Hence the $\bar{U} g_\alpha$ are disjoint and therefore, since they have non-empty interiors and G satisfies the second axiom of countability, it follows that $\{\bar{U} g_\alpha\}$ is a countable set. Now since ϕ is one-to-one, $\{X \cap \phi(\bar{U} g_\alpha)\}$ is a countable disjoint covering of X. Moreover since $\bar{U}$ is closed and included in V it is compact. Hence each $\bar{U} g_\alpha$ is compact, so each $\phi(\bar{U} g_\alpha)$ is compact, so each $X \cap \phi(\bar{U} g_\alpha)$ is closed in X. Now $X \cap \phi(\bar{U} e_G)$ is not empty, and in fact contains e_H. Since X is arcwise connected it follows from (2.2) that $X \cap \phi(\bar{U}) = X$. Thus $X \subseteq \phi(\bar{U}) \subseteq \phi(\bar{U}^2) \subseteq \phi(V)$ so $\phi(V)$ is a neighborhood of e_H as was to be proved.

4. 2. THEOREM. *Let $\mathfrak{G}$ be a locally arcwise connected, locally compact group satisfying the second axiom of countability. If the underlying group of $\mathfrak{G}$ is a topological group $\mathfrak{G}^*$ in a topology weaker than the topology of $\mathfrak{G}$, then $\mathfrak{G}$ is the associated locally arcwise connected group of $\mathfrak{G}^*$. In particular, $\mathfrak{G}^*$ is locally arcwise connected, then $\mathfrak{G} = \mathfrak{G}^*$. In any case the arc components of open subspaces of $\mathfrak{G}^*$ form a base for the topology of $\mathfrak{G}$ and both $\mathfrak{G}$ and $\mathfrak{G}^*$ have the same one-parameter subgroups.*

Proof. Let $\mathcal{G}^{**}$ be the associated locally arcwise connected group of $\mathcal{G}^{*}$. Since, by definition, the topology of $\mathcal{G}^{**}$ is the weakest locally arcwise connected topology stronger than the topology of $\mathcal{G}^{*}$, it follows that the topology of $\mathcal{G}$ is stronger than the topology of $\mathcal{G}^{**}$, i. e., the identity map ϕ is a representation of $\mathcal{G}$ on $\mathcal{G}^{**}$. It follows from (4.1) that ϕ is an isomorphism of $\mathcal{G}$ with $\mathcal{G}^{**}$, i. e. $\mathcal{G} = \mathcal{G}^{**}$.

4.3. COROLLARY. *If $\mathcal{G} = (G, \mathcal{T})$ is a Lie group satisfying the second axiom of countability, then the topology $\mathcal{T}$ of $\mathcal{G}$ is minimal in the set of all locally arcwise connected group topologies for G.*

5. The compact-open and modified compact-open topologies.

Let X be a topological space and let $\mathcal{H}(X)$ denote the group of all homeomorphisms of X on itself. Given subsets of X $K_1, \cdots, K_n$ and $\mathcal{O}_1, \cdots, \mathcal{O}_n$ with the K_i compact and the $\mathcal{O}_i$ open define

$$(K_1, \cdots, K_n; \mathcal{O}_1, \cdots, \mathcal{O}_n) = \{h \in \mathcal{H}(X) : h(K_i) \subseteq \mathcal{O}_i, i = 1, \cdots, n\}.$$

The compact-open topology for $\mathcal{H}(X)$ is by definition the topology in which sets of the above form are a basis. If H is a subgroup of $\mathcal{H}(X)$, then the compact-open topology for H is the topology induced on H by the compact-open topology for $\mathcal{H}(X)$; equivalently it is the topology which has as a basis sets of the form

$$(K_1, \cdots, K_n; \mathcal{O}_1, \cdots, \mathcal{O}_n)_H = \{h \in H : h(K_i) \subseteq \mathcal{O}_i, i = 1, \cdots, n\}.$$

We refer the reader to [1] for details concerning the compact-open topology (it is called the k-topology there). We will need the following facts proved in [1].

5.1. *If X is locally compact, then the compact-open topology for a group of homeomorphisms of X is admissibly strong and is weaker than any other admissibly strong topology.*

5.2. *If X is locally compact and locally connected, then every group of homeomorphisms of X is a topological group in its compact-open topology.*

Immediate from the definition of the compact-open topology is

5.3. PROPOSITION. *If H is a group of homeomorphisms of a space and G a subgroup of H, then the compact-open topology for H induces on G the compact-open topology for G.*.

Another fact we will need is

5.4. Proposition. *If X is a locally compact space satisfying the second axiom of countability, then the compact-open topology for any group H of homeomorphisms of X also satisfies the second axiom of countability.*

Proof. Choose a basis for the topology of X consisting of a sequence $\{\mathcal{O}_i\}$ such that each $\bar{\mathcal{O}}_i$ is compact. Then sets of the form $(\bar{\mathcal{O}}_{i_1}, \cdots, \bar{\mathcal{O}}_{i_n}; \mathcal{O}_{j_1}, \cdots, \mathcal{O}_{j_n})_H$ give a countable base for the compact-open topology for H.

If $\mathfrak{G}$ is a topological group, then the bilateral uniform structure for $\mathfrak{G}$ is that uniform structure generated by uniformities of the form $\{(g,h) \in \mathfrak{G} \times \mathfrak{G} : gh^{-1} \text{ and } g^{-1}h \in V\}$ for some neighborhood V of the indentity in $\mathfrak{G}$. Like the left and right uniform structures for $\mathfrak{G}$ the bilateral uniform structure is compatible with the topology of $\mathfrak{G}$. It has a countable base, and is hence equivalent to a metric, if and only if $\mathfrak{G}$ satisfies the first axiom of countability. Now in [1] Arens shows that if X is a locally compact, locally connected space and $\mathfrak{H}(X)$ is the group of all homeomorphisms of X made into a topological group (5.2) by giving it its compact-open topology, then $\mathfrak{H}(X)$ is complete in its bilateral uniform structure (but not generally in its left and right uniform structures). If we now assume that X satisfies the second axiom of countability and use (5.4), we get a fact mentioned in a footnote of [1].

5.5. Proposition. *Let X be a locally compact, locally connected space satisfying the second axiom of countability and let H be a group of homeomorphisms of X which is closed, relative to the compact-open topology, in the group of all homeomorphism of X. Then the compact-open topology for H can be derived from a complete metric, hence H is of the second category in its compact-open topology.*

Now it is a well-known fact that a continuous one-to-one homomorphism of a locally compact topological group G satisfying the second axiom of countability onto a topological group H of the second category is necessarily bicontinuous (see, for example, Theorem XIII, page 65 of Pontrjagin's *Topological Groups,* where the proof is given under the assumption that H is locally compact, but only the consequence, that H is of the second category, is actually used). Using this result together with (5.1) and (5.5) we get:

5.6. Proposition. *Let X be a locally compact, locally connected space satisfying the second axiom of countability and let H be a group of homeomorphisms of X which is closed, relative to the compact-open topology, in the group of all homeomorphisms of X. If H is a topological group in an admissibly strong, locally compact topology $\mathfrak{T}$ which satisfies the second axiom of countability, then $\mathfrak{T}$ is the compact-open topology for H.*

5.7. PROPOSITION. *Let X be a locally compact space, G a topological group, and ϕ an action of G on X whose range lies in a group H of homeomorphisms of X. Then ϕ is a continuous map of G into H when the latter is given its compact-open topology.*

Proof. Let K be the kernel of ϕ. It follows from the fact that ϕ is an action that K is closed in G. Let h be the canonical homomorphism of G on G/K and $\phi = \tilde{\phi} \circ h$ the canonical factoring of ϕ. Since h is continuous, it will suffice to show that $\tilde{\phi}$ is continuous when H is given its compact-open topology. Now it follows from the fact that h is an open mapping that $\tilde{\phi}$ is an action of G/K on X and of course $\tilde{\phi}$ is one-to-one. Thus it suffices to prove the theorem when ϕ is one-to-one (i.e., effective in the usual terminology). It is then no loss of generality to assume that G is a subgroup of H and that ϕ is the injection mapping. We can then restate the proposition as follows: if the topology of G is admissibly strong it is stronger than the topology induced on G by the compact-open topology of H. Since by (5.3) H induces the compact-open topology on G, this restatement is a consequence of (5.1).

Taking $G = R$ in (5.7) and recalling the definition of admissibly weak we have.

5.8. COROLLARY. *If X is a locally compact space, then the compact-open topology for a group of homeomorphisms of X is always admissibly weak.*

5.9. *Definition.* Let G be a group of homeomorphisms of a space X. the *modified compact-open topology* for G is the topology resulting from applying the operation $\mathfrak{M}$ (3.1) to the compact-open topology for G. In other words it is the topology for G in which the arc components of open subspaces of G (relative to the compact-open topology) form a base.

A word of caution: since the operation $\mathfrak{M}$ does not in general commute with the operation of inducing a topology on a subspace, there is no analogue of (5.3) for the modified compact-open topology, i.e., the modified compact-open topology for a group H of homeomorphisms des not in general induce on a subgroup G of H the modified compact-open topology for G.

5.10. PROPOSITION. *If X is a locally compact space and G is a group of homeomorphisms of X, then the modified compact-open topology for G can be characterized as the weakest admissibly strong topology for G which is locally arcwise connected. Moreover, the modified compact-open topology for G is also admissibly weak.*

Proof. The first conclusion follows from (5.1) and (3.2(3)). If ϕ is an action of R on X with range in G, then by (5.7) ϕ is continuous when G is given its compact-open topology and hence by (3.2(2)) when G is given its modified compact-open topology, i.e., the modified compact-open topology for G is admissibly weak.

5.11. PROPOSITION. *Let X be a locally compact space and G a group of homeomorphisms of X. Then the modified compact-open topology is a Lie topology for G if and only if it makes G a Lie group. The same is true of the compact-open topology.*

Proof. This follows directly from the definition of a Lie topology (1.4) since we have seen (5.1, 5.8, 5.10) that both the compact-open and modified compact-open topologies are admissibly strong and admissibly weak.

5.12. PROPOSITION. *Let G be a group of homeomorphisms of a locally compact, locally connected space X. Then G is a locally arcwise connected topological group in its modified compact-open topology. Moreover, G has the same one-parameter subgroups when given either its compact-open topology or its modified compact-open topology, in fact, in each case they are exactly the actions of R on X with range in G.*

Proof. The first conclusion follows from (5.2) and (3.2(5)). Since we have seen that both the compact-open and modified compact-open topologies are admissibly weak and admissibly strong, the final conclusion follows from (1.2).

5.13. PROPOSITION. *If X is a locally compact space satisfying the second axiom of countability, then the modified compact-open topology for any group of homeomorphisms of X satisfies the first axiom of countability.*

Proof. (5.4) and (3.2(1)).

In general, however, it will not be true in the above case that the modified compact-open topology, like the compact-open topology, satisfies the second axiom of countability.

The following is one of our main results concerning Lie transformation groups.

5.14. THEOREM. *Let $\mathfrak{G} = (G, \mathfrak{T})$ be a Lie group satisfying the second axiom of countability whose underlying group G is a group of homeomorphisms of a locally compact, locally connected space X. If the topology $\mathfrak{T}$ of $\mathfrak{G}$ is admissibly strong, then it is automatically admissibly weak and hence G is a Lie transformation group of X and $\mathfrak{T}$ its Lie topology. Moreover $\mathfrak{T}$*

is the modified compact-open topology for G and if X satisfies the second axiom of countability and G is closed, relative to the compact-open topology, in the group of all homeomorphisms of X, then $\mathcal{J}$ is the compact-open topology for G.

Proof. Since by (5.10) the modified compact-open topology for G is admissibly weak, everything will follow once we show that $\mathcal{J}$ is the modified compact-open topology (the final conclusion is a consequence of (5.6)).

Let $\mathfrak{G}^*$ denote G taken with the modified compact-open topology. By (5.12) $\mathfrak{G}^*$ is a locally arcwise connected topological group. Since $\mathfrak{G}$ is locally arcwise connected and has an admissibly strong topology, it follows from (5.10) that the topology of $\mathfrak{G}$ is stronger than the topology of $\mathfrak{G}^*$. Then by (4.3) $\mathfrak{G} = \mathfrak{G}^*$, i.e., $\mathcal{J}$ is the modified compact-open topology for G.

5.15. COROLLARY. *If a Lie topology for a group G of homeomorphisms of a locally compact, locally connected space satisfies the second axiom of countability, then it is the modified compact-open topology for G.*

5.16. COROLLARY. *If X is a locally compact, locally connected space, then the connected Lie transformation groups of X are precisely the groups of homeomorphisms of X which are connected Lie groups in their modified compact-open topology.*

Proof. (5.11) gives one part of the equivalence and, since a connected Lie group satisfies the second axiom of countability, (5.15) gives the other.

It is not possible in (5.14) to drop the assumption that $\mathfrak{G}$ satisfies the second axiom of countability. For example, if G is a non-trivial connected Lie transformation group of a locally compact, locally connected space X, then in the discrete topology G would satisfy the hypotheses, but not the conclusion of (5.14). This shows that Theorem 9 of [1] is false as stated. The latter states a result similar to part of (5.14) in a special case. It is probably true when the second axiom of countabiilty is added as an assumption on the group G, however, the simple (but invalid) analytical proof given seems irreparable and topological arguments of the type we have used seem necessary.

6. Some dimension theory. In what follows a space stated to have dimension, finite or infinite, is assumed to have a separable metric topology. This is so that all the theorems of [3] will be valid. If X is a compact space and C a closed subset of X, then $H^q(X, C)$ will denote the q-dimensional Cêch cohomology group of X modulo C, and $\Pi^q(X, C)$ will denote the q-dimensional cohomotopy classes of X relative to C, i.e., the homotopy classes of mappings of X into the q-sphere S^q which carry C into the north pole p_0. We wish first to show that if $\dim X = q > 0$, then these two sets are in one-to-one correspondence. Recall first that if $c \in X$ and $q > 0$, then $H^q(X, \{c\})$ is isomorphic to $H^q(X) = H^q(X, \emptyset)$ and that $\Pi^q(X, \{c\})$ is clearly in one-to-one correspondence with $\Pi^q(X) = \Pi^q(X, \emptyset)$. Now let $\tilde{X}$ be the space formed by identifying the closed subset C of the compact space X to a single point c, and let f be the natural projection of X on $\tilde{X}$. Then f is a relative homeomorphism of (X, C) on $(\tilde{X}, \{c\})$, so, by Theorem 5.4, pages 266 of [2], f^* is an isomorphism of $H^q(\tilde{X}; \{s\})$ with $H^q(X, C)$. It is also clear that $\Pi^q(X, \{C\})$ is in natural one-to-one correspondence with $\Pi^q(\tilde{X}, \{c\})$. Now suppose $\dim X = n < \infty$. Then $\dim(\tilde{X} - \{c\}) = \dim(X - C) \leqq n$ so, by Corollary 2, page 32 of [3], $\dim \tilde{X} \leqq n$. Now if $\dim \tilde{X} < n$, both $H^n(\tilde{X})$ and $\Pi^n(\tilde{X})$ contain just one point, while if $\dim \tilde{X} = n$, then $H^n(\tilde{X})$ and $\Pi^n(\tilde{X})$ are in one-to-one correspondence by Theorem VIII 2, page 149 of [3]. Suppose now that $n > 0$ and let us put all these one-to-one correspondences together:

$$H^n(X, C) \leftrightarrow H^n(\tilde{X}, \{c\}) \leftrightarrow H^n(\tilde{X}) \leftrightarrow \Pi^n(\tilde{X}) \leftrightarrow \Pi^n(\tilde{X}, \{c\}) \leftrightarrow \Pi^n(X, C).$$

6.1. LEMMA. *If X is a compact space of dimension n $(0 < n < \infty)$, then there is a one-to-one correspondence between $H^n(X, C)$ and $\Pi^n(X, C)$.*

6.2. THEOREM. *Let X be a compact space of finite dimension $n > 0$. Then there is a closed subset C of X for which there exists an essential map of the pair (X, C) into (S^n, p_0).*

Proof. Since the inessential maps of (X, C) into (S^n, p_0) are just those in the same homotopy class as the constant map $\tilde{p}_0$, it suffices to show that $\Pi^n(X, C)$ contains more than one element for some closed subset C of X. In view of the lemma it suffices to find a closed subset C of X for which $H^n(X, C) \neq 0$. But if on the contrary $H^n(X, C) = 0$ for all closed subsets C of X, then it would follow from Theorem VIII 4, page 152 of [3] that $\dim X \leqq n - 1$, a contradiction.

6.3. BORSUK'S THEOREM. *Let Y be a closed subspace of a space X and C a closed subspace of Y. Let f and g be homotopic mappings of (Y, C) into (S^n, p_0). If f has an extension F over X relative to S^n, then there is an extension G of g over X such that F and G are homotopic mappings of (X, C) into (S^n, p_0).*

Proof. This is stated and proved as Theorem VI 5, page 86 of [3] for the case $C = \emptyset$. However the proof given actually proves the more general relativized form stated above.

6.4. LEMMA. *Let Y be a closed subset of a space X and C a closed subset of Y. Let F be a map of (X, C) into (S^n, p_0) such that f, the restriction of F to Y, is an inessential map of (Y, C) into (S^n, p_0). Then there is a neighborhood V of Y such that the restriction of F to V is an inessential map of (V, C) into (S^n, p_0).*

Proof. Let g be the constant map $y \to p_0$ of (Y, C) into (S^n, p_0). By assumption f and g are homotopic mappings of (Y, C) into (S^n, p_0), hence by (6.3) there is an extension G of g over X such that F and G are in the same homotopy class as mappings of (X, C) into (S^n, p_0). *A fortiori* if V is any neighborhood of Y, then the restrictions of F and G to V are homotopic maps of (V, C) into (S^n, p_0), hence it suffices to find a neighborhood V of Y for which G restricted to V is an inessential map of (V, C) into (S^n, p_0). But clearly if U is any contractible neighborhood of p_0 on S^n then $G^{-1}(U) = V$ works.

The following result, or at least closely related ones, are known. However the proof is short and we include it for completeness.

6.5. THEOREM. *Let C be a closed subspace of a compact space X and let f be an essential map of the pair (X, C) into (S^n, p_0). Then the family $\mathfrak{F}$ of closed subsets Y of X which include C and for which the restriction of f to Y is an essential map of (Y, C) into (S^n, p_0) contains a minimal element.*

Proof. By Zorn's lemma it suffices to show that the ordering of $\mathfrak{F}$ by inclusion is inductive, i.e., if Γ is a chain in $\mathfrak{F}$ and F is the intersection of the elements of Γ, then we must show that $F \in \mathfrak{F}$. Suppose on the contrary that $F \notin \mathfrak{F}$. Since clearly $C \subseteq F$ this means that f restricted to F is an inessential map of (F, C) into (S^n, p_0) and hence by (6.4) there is an open set V including F such that f restricted to V is an inessential map of (V, C) into (S^n, p_0). Now $\{Y - V : Y \in \Gamma\}$ is a chain of compact sets with empty intersection and hence $Y - V$ is empty for some $Y \in \Gamma$. But then $Y \subseteq V$ and hence the restriction of f to Y is an inessential map of (Y, C) into (S^n, p_0) so $Y \notin \mathfrak{F}$, contradicting $\Gamma \subseteq \mathfrak{F}$.

7. A criterion for Lie groups.

This section contains the proof of a theorem reported by one of the authors in [4].

7.1. THEOREM. *Let G be a locally arcwise connected topological group. If X is a non-void compact, metrizable subspace of G of dimension $n < \infty$, then either X has an interior point or else there is an arc A in G such that AX is compact, metrizable and of dimension greater than n.*

Proof. We note first that if A is any arc in G, then AX is compact and metrizable. In fact, A is the continuous image of the unit interval I under some map σ so that AX is the continuous image of the compact, metrizable space $I \times X$ under the continuous map $(t, x) \rightarrow \sigma(t)x$. The desired result now follows from Satz IX, § 3, Chapter II of [7].

If $n = 0$ then either G is discrete, in which case every point of X is an interior point, or else G has a non-trivial arc A in which case AX has a non-trivial arc and therefore is of dimension greater than or equal to one.

Now suppose $n > 0$. By (6.2) we can find a closed subset C of X for which there exists an essential map f of the pair (X, C) into (S^n, p_0). By (6.5) there is a closed subset X' of X including C such that f restricted to X' is an essential map of the pair (X', C) into (S^n, p_0), but for any non-void open subset U of X' disjoint from C the restriction of f to $X' - U$ is an inessential map of $(X' - U, C)$ onto (S^n, p_0). Without loss of generality we can assume that $e \in X' - C$, for in any case this can be arranged by a translation.

Let V be an arcwise connected neighborhood of e such that $V^{-1}\bar{V}$ is disjoint from C. Suppose now that X has no interior points. Then certainly V^{-1} is not included in X', so we can find a continuous map σ of the unit interval into G such that $\sigma(0) = e$, $A =$ range of $\sigma \subseteq V$, and $\sigma(1)^{-1} \notin X'$. Then $e \notin \sigma(1)X'$, hence since X' is compact, we can find an open neighborhood U of e with $U \subseteq V$ and $\bar{U}$ disjoint from $\sigma(1)X'$. By the choice of X' the restriction of f to $X' - U$ is homotopic, as a map of the pair $(X' - U, C)$ into (S^n, p_0), to the constant mapping $x \rightarrow p_0$. By (6.3) it follows that there is a map g of the pair (X', C) into (S^n, p_0) such that $g(x) = p_0$ for $x \in X' - U$ which is homotopic to the restriction of f to X' and therefore is essential.

Now note that $AC \cup \sigma(1)X'$ is disjoint from $\bar{U}$. In fact, $\bar{U}$ was chosen disjoint from $\sigma(1)X'$ while, since $A \subseteq V$ and $V^{-1}\bar{V}$ is disjoint from C, it follows that AC is disjoint from $\bar{V}$ and *a fortiori* from $\bar{U}$. Then since $g(x) = p_0$ for $x \in X' - U$, it follows that the defining conditions $h(x) = p_0$ for $x \in AC \cup \sigma(1)X'$, $h(x) = g(x)$ for $x \in X'$ are non-contradictory and define a continuous mapping h of $X' \cup AC \cup \sigma(1)X'$ into S^n. It follows from the essentiality of g that h does not have a continuous extension over

AX' relative to S^n. In fact, if $\bar{h}$ were such an extension of h, then $H: I \times X' \rightarrow S^n$, defined by $H(t,x) = \bar{h}(\sigma(t)x)$ would be a homotopy of g (considered as a map of the pair (X', C) into (S^n, p_0)) with the constant map $x \rightarrow p_0$. It follows *a fortiori* that h does not have a continuous extension over AX relative to S^n. Since as we have already seen AX is metrizable, we can apply the theorems of [3]. In particular, by Theorem VI 4, page 83 of [3], the existence of a continuous mapping of a closed subspace of AX into S^n which does not admit a continuous extension over all of AX implies that $\dim(AX) > n$.

7.2. THEOREM. *A locally arcwise connected topological group G in which the compact metrizable subspaces are of bounded dimension is a Lie group.*

Proof. Let n be the least upper bound of the dimensions of the compact, metrizable subspaces of G and let X be a compact metrizable subspace of G of dimension n. By (7.1) X has an interior point g. Then $V = g^{-1}X$ is a compact n-dimensional neighborhood of the identity in G. Hence G is a locally connected, locally compact, n-dimensional topological group and, by the theorem on page 185 of [5], G is a Lie group.

7.3. COROLLARY. *If G is a topological group in which the compact, metrizable subspaces are of bounded dimension, then the associated locally arcwise connected group of G (Definition 3.3) is a Lie group.*

Proof. Since the topology of G^*, the associated locally arcwise connected group of G, is stronger than the topology of G, the compact metrizable subspaces of G^* are also compact metrizable subspaces of G and hence have bounded dimension.

7.4. COROLLARY. *Let G be a topological group in which some neighborhood of the identity admits a continuous one-to-one map into a finite dimensional metric space. Then the associated locally arcwise connected group of G is a Lie group and in particular if G is locally arcwise connected, then G is a Lie group.*

Proof. Let f be a continuous one-to-one map of a closed neighborhood V of the identity into a finite dimensional metric space X. Given a compact subspace K of G and $k \in K$, $kV \cap K$ is a compact neighborhood of k in K. The map $h \rightarrow f(k^{-1}h)$ maps $kV \cap K$ homeomorphically onto a compact subspace of X. It follows that $kV \cap K$ is of dimension less than or equal to n. Since each point of K has a neighborhood of dimension less than or equal to n, it follows that $\dim(K) \leqq n$ and (7.4) now follows from (7.3).

8. A criterion for Lie transformation groups.

8.1. *Definition.* A set Φ of homeomorphisms of a space X will be said to be *faithfully represented* by a subset F of X if $\phi \in \Phi$ and $\phi(x) = x$ for all $x \in F$ implies ϕ is the identity map of X.

8.2. THEOREM. *Let $\mathfrak{G} = (G, \mathfrak{T})$ be a Lie group whose underlying group G is a group of homeomorphism of a space X and whose topology $\mathfrak{T}$ is admissibly strong. Then some neighborhood of the identity in $\mathfrak{G}$ is faithfully repersented by a finite subset F of X. In fact, if* $\dim \mathfrak{G} = n$ *then F can be taken to have n or fewer points.*

Proof. Given a finite subset F of X, let

$$G_F = \{g \in G \colon g(x) = x \text{ for all } x \in F\}.$$

Each G_F is a closed subgroup of $\mathfrak{G}$ and hence a Lie group. It will suffice to prove that for some F containing n or fewer points, G_F is zero-dimensional and hence discrete. We prove this by showing that if $\dim G_F > 0$, then for some $x \in X$ we have $\dim G_{F \cup \{x\}} < \dim G_F$. In fact, let $\phi \colon t \rightarrow \phi_t$ be a non-trivial one-parameter subgroup of G_F and let t be a real number such that $\phi_t \neq e$. Choose $x \in X$ such that $\phi_t(x) \neq x$. Then $G_{F \cup \{x\}}$ is a subgroup of G_F and ϕ is a one-parameter subgroup of G_F but not of $G_{F \cup \{x\}}$.

There is a partial converse to (8.2), namely,

8.3. THEOREM. *Let $\mathfrak{G} = (G, \mathfrak{T})$ be a topological group whose underlying group G is a group of homeomorphisms of a finite dimensional metric space X and whose topology $\mathfrak{T}$ is admissibly strong. If some neighborhood of the identity in $\mathfrak{G}$ is faithfully represented by a finite subset of X, then the associated locally arcwise connected group of $\mathfrak{G}$ is a Lie group, and in particular if $\mathfrak{G}$ is locally arcwise connected, it is a Lie group.*

Proof. Let U be a neighborhood of the identity in $\mathfrak{G}$ faithfully represented by a finite subset $x_1, \cdots, x_n$ of X and choose a neighborhood V of the identity with $V^{-1}V \subseteq U$. Then $f \colon g \rightarrow (g(x_1), \cdots, g(x_n))$ is a continuous map of V into X^n. Moreover, if $f(g) = f(h)$ for $g, h \in V$ then $g^{-1}h(x_i) = g^{-1}g(x_i) = x_i$, $i = 1, 2, \cdots, n$; since $g^{-1}h \in U$, it follows that $g^{-1}h = e$ or $g = h$. Thus f is one-to-one and since $\dim X^n \leqq n \dim X < \infty$, the proposition follows from (7.4).

8.4. THEOREM. *Let X be a locally compact, locally connected, finite dimensional metric space. A necessary and sufficient condition for a group G of homeomorphisms of X to be a Lie transformation group of X with the* *modified compact-open topology as its Lie topology is that some modified compact-open neighborhood of the identity in G be faithfully represented by a finite subset of X.*

Proof. Necessity follows from (8.2). Since the modified compact-open topology for G is admissibly strong (5.10) and makes G a locally arcwise connected topological group (5.12), sufficiency follows from (8.3).

Since the modified compact-open neighborhoods of the identity are generally impossible to determine while the compact-open neighborhoods of the identity are explicitly given, the following corollary to (8.4) is a more useful criterion than the theorem itself.

8.5. COROLLARY. *Let G be a group of homeomorphisms of a locally compact, locally connected, finite dimensional metric space X. If some compact-open neighborhood of the identity in G is faithfully represented by a finite subset of X, then G is a Lie transformation group of X and the modified compact-open topology for G is its Lie topology. In particular, if G itself is faithfully represented by a finite subset of X, it is a Lie transformation group of X with the modified compact-open topology as its Lie topology.*

Proof. A compact-open neighborhood of the identity in G is *a fortiori* a modified compact-open neighborhood of the identity.

It is perhaps in order here to remark on the relevance (or rather irrelevance) of the various metrizability assumptions we have made in Section 6 and thereafter. In general these have been made to justify the use made of theorems proved in [3], where all spaces are taken to be separable metric. However, since all the spaces to which dimension arguments are directly applied are, in this paper, compact, it is possible as the referee suggests to use the Lebesque definition of dimension in terms of the minimum number of interesecting sets in small open coverings, and drop all references to metrizability. For the results in Section 6 and for Theorem 7.1 this would strengthen our results. However for the main theorem, Theorem 7.2, dropping the reference to metrizability would at least formally weaken the theorem. Using the referee's suggestion, Corollary 7.4 can be strengthened by replacing metric by compact in its statement. That this gives a really stronger result follows from the fact that a finite dimensional metric space can be imbedded in a finite dimensional compact space. In fact the referee notes that locally compact can replace metric in Corollary 7.4, provided the dimension of a locally compact space is defined as the supremum of the dimensions of its compact subspaces. This is immediate from the proof of this corollary. Having noted this last fact it follows that in Theorems 8.3 and 8.4 and in Corollary 8.5 we can drop the assumption that X is metric.

9. A conjecture. Let X be a connected manifold satisfying the second axiom of countability. Let G be a connected Lie transformation group of X, or what is the same (5.16), a group of homeomorphisms of X that is a connected Lie group in its modified compact-open topology. Let $\bar{G}$ be the closure of G, relative to the compact-open topology, in the group of all homeomorphisms of X. Then we conjecture that $\bar{G}$ is also a Lie transformation group of X and that the Lie topology of $\bar{G}$ is its compact-open topology.

If this is so, then the structure of the class of connected Lie transformation groups of X is very clear. On the one hand, there are those groups of homeomorphisms of X which are connected Lie groups in their compact-open topology, and all others are analytic subgroups of these. The validity of this structure theorem would have many interesting consequences.

If M is a differentiable manifold with X as its underlying topological manifold, then we define a Lie transformation group of M to be a Lie transformation group of X consisting entirely of differentiable homeomorphisms. The differentiable structure of M allows one to develop an infinitesimal characterization of Lie transformation groups of M in terms of vector fields on M. This is carried out by one of the authors in a recent Memoir of the American Mathematical Society [6].

HARVARD UNIVERSITY.

REFERENCES.

[1] R. F. Arens, "Topologies for homeomorphism groups," *American Journal of Mathematics*, vol. 68 (1946), pp. 593-610.

[2] S. Eilenberg and N. Steenrod, *Foundations of Algebraic Topology*, Princeton, 1952.

[3] W. Hurewicz and H. Wallman, *Dimension Theory*, Princeton, 1948.

[4] A. M. Gleason, "Arcs in locally compact groups," *Proceedings of the National Academy of Sciences*, vol. 38 (1950), pp. 663-667.

[5] D. Montgomery and L. Zippin, *Topological Transformation Groups*, Interscience, New York, 1955.

[6] R. S. Palais, *A Global Formulation of the Lie Theory of Transformation Groups*, Memoirs of the American Mathematical Society 22, 1957.

[7] P. Alexandroff and H. Hopf, *Topologie*, I, Berlin, Springer, 1935.

[8] N. Bourbaki, *Topology Générale*, Chapt. IX, Hermann, Paris, 1948.

composition in A. Specifically, this means the following. Let G be the graph of the law of composition in A, so that G is a subvariety in $A \times A \times A$; then our condition can be expressed by saying that both $\bar{A}$ and $\bar{G}$ are varieties (in $\bar{S}^n$ and $\bar{S}^n \times \bar{S}^n \times \bar{S}^n$ respectively) and that $\bar{G}$ defines an abelian law of composition in $\bar{A}$. We observe that if e is the unit element in A, then $\bar{e}$ is the unit element in $\bar{A}$; in fact, e is characterized by the condition that $\mathrm{pr}_{32}(e \times A \times A))$ is contained in the diagonal in $A \times A$, and this condition is evidently preserved under the specialization.

THEOREM 1. *Let A and B be abelian varieties in S^n, and let T be a birational isomorphism between A and B; we assume that A, B, and T are all defined over k. If the specializations $\bar{A}$ and $\bar{B}$ are non-degenerate, then the specialization $\bar{T}$ is a variety and defines a birational isomorphism between $\bar{A}$ and $\bar{B}$.*

Proof. It is clear that $\bar{A} \times \bar{B}$ is the specialization of $A \times B$ and is non-degenerate. If we denote the graph of T by the same symbol, then the support $|\bar{T}|$ of $\bar{T}$ is an algebraic subgroup in $\bar{A} \times \bar{B}$; this follows from the fact that T is an abelian subvariety in $A \times B$, and the fact that the law of composition in $\bar{A} \times \bar{B}$ is the specialization of the law of composition in $A \times B$. Let $\bar{T}_0$ be a component in $\bar{T}$ which contains the unit element; then $\bar{T}_0$ is an abelian subvariety in $\bar{A} \times \bar{B}$, and every component in $|\bar{T}|$ and hence also every component in $\bar{T}$ is obtained from $\bar{T}_0$ by a translation. By assumption, we have $\mathrm{pr}_1 T = A$ and $\mathrm{pr}_2 T = B$; hence, by specialization, we have $\mathrm{pr}_1 \bar{T} = \bar{A}$ and $\mathrm{pr}_2 \bar{T} = \bar{B}$. Since all cycles obtained from $\bar{T}_0$ by translations must have the same projections on $\bar{A}$ and $\bar{B}$, we conclude readily that $\mathrm{pr}_1 \bar{T}_0 = \bar{A}$ and $\mathrm{pr}_2 \bar{T} = \bar{B}$, and that $\bar{T}_0$ is the only component in $\bar{T}$ and has the coefficient 1. This shows that $\bar{T} = \bar{T}_0$ defines a birational transformation between $\bar{A}$ and $\bar{B}$, which, since it preserves the unit elements, must be an isomorphism.

We turn now to the case of the curves C_1 and C_2 considered at the beginning of this note. Let C be a non-singular curve of genus $g(C)$ in S^n, defined over k; we shall say that the specialization $\bar{C}$ is *non-degenerate* if $\bar{C}$ is a non-singular curve and hence has the same genus $g(C)$ as C. We assume that there exists a birational correspondence F between C_1 and C_2, defined over k, and that the specialization $\bar{C}_1$ and $\bar{C}_2$ are both non-degenerate. Since the conditions $\mathrm{pr}_1 F = C_1$ and $\mathrm{pr}_2 F = C_2$ imply by specialization the conditions $\mathrm{pr}_1 \bar{F} = \bar{C}_1$ and $\mathrm{pr}_2 \bar{F} = \bar{C}_2$, we conclude that $\bar{F}$ is either a birational correspondence between $\bar{C}_1$ and $\bar{C}_2$, or has the form $x \times \bar{C}_2 + \bar{C}_1 \times y$, for some points x and y in $\bar{C}_1$ and $\bar{C}_2$ respectively. In case $g(C_1) = g(C_2) = 0$, it can be easily seen by examples that both possibilities can occur; however, in this case the assertion of Deuring is trivially true. In the next theorem we shall show that, except in this trivial case, the second possibility cannot occur; this implies that the specialization $\bar{F}$ is itself already such a birational correspondence.

THEOREM 2. *Let C_1 and C_2 be non-singular curves of genus > 0 in S^n, and let F be a birational correspondence between C_1 and C_2; we assume that C_1, C_2, and F are all defined over k. If the specializations $\bar{C}_1$ and $\bar{C}_2$ are non-degenerate, then the specialization $\bar{F}$ is a birational correspondance between $\bar{C}_1$ and $\bar{C}_2$.*

Proof. The theorem being "geometric," we may assume that the curves C_1 and C_2 have rational points over k, and hence the curves $\bar{C}_1$ and $\bar{C}_2$ have rational points over $\bar{k}$. In fact, we can enlarge k by a finite algebraic extension if necessary, and extend the discrete valuation in k to a discrete valuation of this extension; it is easily seen that the validity of our theorem over this extension will imply its validity in the original form.

For $i = 1, 2$, we consider the Jacobian J_i of C_i and the canonical mapping f_i of C_i into J_i with reference to a rational point p_i in C_i (i.e., $f_i(p_i) = e_i$, e_i being the unit element in J_i), both J_i and f_i being constructed as in Chow [1]. It is essential for our purpose that J_i *and* f_i are constructed in this particular way, which we shall call the Chow construction, not just some arbitrarily chosen projective models of J_i and the corresponding mapping f_i. The reason lies in the fact that the Chow construction is "compatible" with specializations, at least when they are non-degenerate. Specifically, this means that if the specialization $\bar{C}_i$ is non-degenerate, then the specialization $\bar{J}_i$ (which is a cycle in $\bar{S}^{t_i}$ if S^{t_i} is the ambient projective space of J_i) of the abelian variety J_i is also non-degenerate, and $\bar{J}_i$ and $\bar{f}_i$ are respectively the Jacobian and the canonical mapping of $\bar{C}_i$. This fact is a special case of a more general "compatibility" theorem of Igusa [3] (Igusa treats only the algebro-geometric specializations, but it is easily seen that his proof is also valid for the more general specializations considered here at least in the non-degenerate case). For the sake of convenience, we shall assume that $p_2 = F(p_1)$; then there exists a birational isomorphism T between J_1 and J_2, defined over k, such that $T \circ f_1 = f_2 \circ F$. If we denote by f the mapping $f_1 \times f_2$ of $C_1 \times C_2$ into $J_1 \times J_2$, and if we denote the graphs of F and T by the same symbols, then the above relation implies that $f(F)$ is contained in T. Since the specialization $\bar{f} = \bar{f}_1 \times \bar{f}_2$ is a rational mapping of $\bar{C}_1 \times \bar{C}_2$ into $\bar{J}_1 \times \bar{J}_2$, it follows that the cycle $\bar{f}(\bar{F})$ is defined and is contained in $|\bar{T}|$.

By Theorem 1, $\bar{T}$ is an abelian subvariety in $\bar{J}_1 \times \bar{J}_2$ (it is in fact sufficient to know that $|\bar{T}|$ is an algebraic group in $\bar{J}_1 \times \bar{J}_2$) and is a proper subset in $\bar{J}_1 \times \bar{J}_2$. If $\bar{F}$ is not a birational correspondence between $\bar{C}_1$ and $\bar{C}_2$, then by a previous remark we must have $\bar{F} = \bar{p}_1 \times \bar{C}_2 + \bar{C}_1 \times \bar{p}_2$ (we observe that $|\bar{F}|$ must contain the point $\bar{p}_1 \times \bar{p}_2$) and hence

$$\bar{f}(\bar{F}) = \bar{e}_1 \times \bar{f}_2(\bar{C}_2) + \bar{f}_1(\bar{C}_1) \times \bar{e}_2.$$

This shows that $|\bar{f}(\bar{F})|$ generates the entire variety $\bar{J}_1 \times \bar{J}_2$, in contradiction to the fact that $\bar{f}(\bar{F})$ is contained in $\bar{T}$. This proves our theorem.

THE JOHNS HOPKINS UNIVERSITY,
COLUMBIA UNIVERSITY.

REFERENCES.

[1] W. L. Chow, "The Jacobian variety of an algebraic curve," *American Journal of Mathematics*, vol. 76 (1954), pp. 453-476.

[2] M. Deuring, "Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins (II)," *Nachrichten der Akademie der Wissenschaften in Göttingen*, 1955, pp. 13-42.

[3] J. Igusa, "Fibre systems of Jacobian varieties," *American Journal of Mathematics*, vol. 78 (1956), pp. 171-199.

[4] G. Shimura, "Reduction of algebraic varieties with respect to a discrete valuation of the basic field," *ibid.*, vol. 77 (1955), pp. 131-176.

FOURIER TRANSFORMS ON A SEMISIMPLE LIE ALGEBRA II.*

By HARISH-CHANDRA.

1. Introduction. The purpose of this paper is to complete the proofs of two results (Theorems 2 and 3) which have already been mentioned in [4(e), § 1]. For the first one, the problem reduces to showing that the constants of the Corollary to Lemma 29 of [4(e)] are all equal. It is obvious that this can be done only by taking the singular elements of $\mathfrak{g}_0$ into account. However, as we shall see, it is enough to consider only the best among these, namely, the semiregular ones (see Section 2). Let $\mathfrak{g}_0'$ be the set of all regular elements in $\mathfrak{g}_0$. We first show that a given semiregular element H_0 of $\mathfrak{g}_0$ can lie in the closure of at most three distinct connected components of $\mathfrak{g}_0'$. Let $\mathfrak{l}_0$ be the real semisimple Lie algebra of dimension 3 spanned by the elements H, X, Y satisfying the relations $[H,X]=2X$, $[H,Y]=-2Y$, $[X,Y]=H$. Then zero is the only semiregular element in $\mathfrak{l}_0$ and certain computations on $\mathfrak{g}_0$ around H_0 can be reduced to similar computations on $\mathfrak{l}_0$ around zero (see Lemma 8 and its Corollary). Now the distribution T' of [4(e), § 7] satisfies certain differential equations [4(e), Lemma 30]. If we transcribe these equations on $\mathfrak{l}_0$, they become simple enough to be handled directly (see Lemma 12). In this way, one proves that T' coincides with a constant on some neighborhood of H_0. Theorem 2 now follows from the fact that the union of regular and semiregular elements of $\mathfrak{g}_0$ is connected (Lemma 13). Once Theorem 2 is proved, Theorem 3 can be obtained without much difficulty from Lemma 41 of [4(e)].

For the convenience of the reader all calculations on $\mathfrak{l}_0$ have been collected together in the Appendix (Section 6).

The main results of this paper have been announced in a short note [4(f)].

2. Transformation of certain integrals. We keep to the notation of [4(d), (e)]. Call an element $X \in \mathfrak{g}$ *semiregular* if (1) $\operatorname{ad} X$ is semisimple and (2) the centralizer of X in $\mathfrak{g}$ is of dimension $l+2$ (where $l = \operatorname{rank} \mathfrak{g}$). Let $\mathfrak{h}_0$ be a Cartan subalgebra of $\mathfrak{g}_0$ such that $\theta(\mathfrak{h}_0)=\mathfrak{h}_0$ and let H_0 be a semiregular element in $\mathfrak{h}_0$. Define P, P_+, P_0 and P_- as in Section 5 of [4(e)]:

---

* Received July 30, 1956.

Then since H_0 is semiregular, it is obvious that $\alpha_0(H_0) = 0$ for exactly one root $\alpha_0 \in P$, and the centralizer of H_0 in $\mathfrak{g}$ is $\mathfrak{z} = \mathfrak{h} + CX_{\alpha_0} + CX_{-\alpha_0}$. Let Q be the set of those roots $\alpha \in P$ for which α^2 takes only real values on $\mathfrak{h}_0$. We claim $\alpha_0 \in Q$. For otherwise, suppose $\alpha_0 \notin Q$ and put $\beta = -\theta\alpha_0$. Then β is also a root and $\beta(H) = \operatorname{conj} \alpha_0(H)$ $(H \in \mathfrak{h}_0)$. This implies that $\beta(H_0) = 0$, and therefore $X_\beta \in \mathfrak{z}$. On the other hand $\beta \neq \pm \alpha_0$ since $\alpha_0 \notin Q$. Therefore it is obvious that $X_\beta \notin \mathfrak{z}$, and we get a contradiction. Hence $\alpha_0 \in Q$. Moreover, it is clear that $\bar{\theta}(\mathfrak{z}) = \mathfrak{z}$, and therefore (see [4(e), Lemma 10]) $\mathfrak{z}$ is reductive in $\mathfrak{g}$ and $\mathfrak{z} = \sigma + \mathfrak{l}$, where σ is the center and $\mathfrak{l} = [\mathfrak{z}, \mathfrak{z}] = CH_{\alpha_0} + CX_{\alpha_0} + CX_{-\alpha_0}$ the derived algebra of $\mathfrak{z}$. Obviously σ is the set of all $H \in \mathfrak{h}$, where $\alpha_0(H) = 0$. Put $\sigma_0 = \sigma \cap \mathfrak{h}_0$. Then $\mathfrak{z}_0 = \mathfrak{z} \cap \mathfrak{g}_0 = \sigma_0 + \mathfrak{l}_0$, where $\mathfrak{l}_0 = \mathfrak{l} \cap \mathfrak{g}_0$. Now $\dim_R \mathfrak{z}_0 = \dim \mathfrak{z} = l + 2$ and $\dim_R \sigma_0 = l - 1$. Hence $\dim_R \mathfrak{l}_0 = 3$, and this shows that $\mathfrak{l}_0$ is a real form of the complex semisimple Lie algebra $\mathfrak{l}$. Put $H_{\alpha_0}' = 2\alpha_0(H_{\alpha_0})^{-1} H_{\alpha_0}$ and define Q_+ as in [4(e), § 12]. We select X_{α_0} and $X_{-\alpha_0}$ in accordance with Corollary 1 of Lemma 46 of [4(e)]. Then $\mathfrak{l}_0 = RH_{\alpha_0}' + RX_{\alpha_0} + RX_{-\alpha_0}$ if $\alpha_0 \in Q_+$ and

$$\mathfrak{l}_0 = R(-1)^{\frac{1}{2}} H_{\alpha_0}' + R(X_{\alpha_0} - X_{-\alpha_0}) + R(-1)^{\frac{1}{2}}(X_{\alpha_0} + X_{-\alpha_0}) \text{ if } \alpha_0 \in P_-.$$

In the latter case, $\mathfrak{l}_0$ is compact (see Section 6). Finally,

$$\mathfrak{l}_0 = R(-1)^{\frac{1}{2}} H_{\alpha_0}' + R(-1)^{\frac{1}{2}}(X_{\alpha_0} - X_{-\alpha_0}) + R(X_{\alpha_0} + X_{-\alpha_0}) \text{ if } \alpha_0 \in P_0.$$

Let $\mathfrak{l}'$ be the set of those points in $\mathfrak{l}$ which are regular (with respect to $\mathfrak{l}$). Put $\mathfrak{l}_0' = \mathfrak{l}' \cap \mathfrak{l}_0$.

Let $\mathfrak{q}$ be the orthogonal complement of $\mathfrak{z}$ in $\mathfrak{g}$. Then $\mathfrak{q} = \sum_{\substack{\alpha \in P \\ \alpha \neq \alpha_0}} (CX_\alpha + CX_{-\alpha})$ and $[\mathfrak{z}, \mathfrak{q}] \subset \mathfrak{q}$. Let $\zeta(Z)$ $(Z \in \mathfrak{z})$ denote the determinant of the restriction of $\operatorname{ad} Z$ on $\mathfrak{q}$. Then ζ is a polynomial function on $\mathfrak{z}$ which takes only real values on $\mathfrak{z}_0$ and $\zeta(H) = (-1)^{r-1} \prod_{\substack{\alpha \in P \\ \alpha \neq \alpha_0}} \alpha(H)^2$ $(H \in \mathfrak{h})$, where r is the number of roots in P. This shows that $\zeta(H_0) \neq 0$. Let $\mathfrak{z}_0'$ be the set of those points $Z \in \mathfrak{z}_0$ where $\zeta(Z) \neq 0$. Select an open connected neighborhood U of H_0 in $\mathfrak{z}_0'$ and consider the factor space $G^* = G/\Xi$, where G is the (connected) adjoint group of $\mathfrak{g}_0$ and Ξ is the centralizer of H_0 in G. We denote by $x \to x^*$ $(x \in G)$ the natural mapping G on G^*. Choose an open connected neighborhood V^* of 1^* in G^*. Then if V^* is sufficiently small, we can define (see Chevalley [2, p. 111]) an analytic mapping ϕ of V^* into G with the following properties: (1) $(\phi(x^*))^* = x^*$ $(x^* \in V^*)$ and (2) ϕ is regular on V^*. Put $V = \phi(V^*)$ and consider the mapping ψ: $(x^*, Z) \to \phi(x^*)Z$ $(x^* \in V^*, Z \in U)$ of $V^* \times U$ into $\mathfrak{g}_0$. We shall prove that ψ is regular. For

$Y \in \mathfrak{g}_0$ and $X^* \in V^*$, put[1] $Y_{x^*}{}^* = d\tau_x(Y)$, where $x = \phi(x^*)$ and τ is the natural mapping of G on G^*. Identify the tangent space of $V^* \times U$ at (x^*, Z) with $\mathfrak{g}_0$ under the linear isomorphism

$$Y + X \leftrightarrow Y_{x^*}{}^* \times X \qquad (Y \in \mathfrak{q}_0, X \in \mathfrak{z}_0).$$

Then a simple calculation shows that

$$d\psi_{x^*,Z}(Y + X) = \phi(x^*)X - \phi(x^*) \operatorname{ad} Z (d\phi_{x^*} Y_{x^*}{}^*).$$

But since $\tau\phi$ is the identity mapping on V^*, $d\tau_x(d\phi_{x^*} Y_{x^*}{}^* - Y) = 0$ if $x = \phi(x^*)$, and therefore $d\phi_{x^*} Y_{x^*}{}^* \equiv Y \bmod \mathfrak{z}_0$. Hence if $D_{x^*,Z} = (\phi(x^*))^{-1} d\psi_{x^*,Z}$, it is clear that

$$D_{x^*,Z}X = X \quad (X \in \mathfrak{z}_0), \qquad D_{x^*,Z}Y \equiv -(\operatorname{ad} Z)Y \quad (Y \in \mathfrak{q}_0),$$

and so we conclude that $|\det(d\psi_{x^*,Z})| = |\det D_{x^*,Z}| = |\zeta(Z)| \neq 0$, since $U \subset \mathfrak{z}_0'$. This proves that ψ is everywhere regular on $V^* \times U$. Therefore, since the dimensions of the two manifolds $V^* \times U$ and $\mathfrak{g}_0$ are equal, it follows that ψ is also open and univalent provided V^* and U are sufficiently small. Put $N = \psi(V^* \times U)$. Then N is an open connected neighborhood of H_0 in $\mathfrak{g}_0$ and ψ defines an analytic isomorphism of $V^* \times U$ with N.

Since $\mathfrak{z}_0$ is reductive, the group Ξ is unimodular, and therefore (see Weil [8, p. 45]) there exists an invariant measure dx^* on G^*. Let dX and dZ denote the Euclidean measures on $\mathfrak{g}_0$ and $\mathfrak{z}_0$, respectively. Then the above calculation shows that dx^* can be so normalized that

$$\int_N f(X)\,dX = \int_{V^* \times U} f(\psi(x^*, Z))\,|\zeta(Z)|\,dx^* dZ \qquad (f \in C_c(N)).$$

Select once for all an element $a_0 \in C_c^\infty(V^*)$ such that $\int a_0(x^*)\,dx^* = 1$, and for any $\gamma \in C_c^\infty(U)$ define $f_\gamma \in C_c^\infty(N)$ by $f_\gamma(\psi(x^*, Z)) = a_0(x^*)\gamma(Z)$ $(x^* \in V^*, Z \in U)$. Then the following result is obvious.

LEMMA 1. *Let $'U$ be any open subset of U and put $'N = \psi(V^* \times {}'U)$. Then*

$$\int_{'N} f_\gamma(X)\,dX = \int_{'U} \gamma\,|\zeta|\,dZ \text{ for all } \gamma \in C_c^\infty('U).$$

On the other hand, it is clear that σ_0 and $\mathfrak{l}_0$ are mutually orthogonal. Let U_σ and $U_{\mathfrak{l}}$, respectively, denote the orthogonal projections of U in σ_0 and $\mathfrak{l}_0$. Then by replacing U, if necessary, by a smaller open connected neighborhood of H_0 in $\mathfrak{z}_0'$, we can assume that (1) $U = U_\sigma + U_{\mathfrak{l}}$, (2) U_σ is convex and $\alpha(H) \neq 0$ for any $H \in U_\sigma$ and $\alpha \neq \alpha_0$ in P, (3) if $Z \in U_{\mathfrak{l}}$ then tZ $(0 \leqq t \leqq 1)$ is also in $U_{\mathfrak{l}}$. Define the polynomial η as in [4(e), § 6] and let $\mathfrak{g}_0'$ be the set of all regular elements in $\mathfrak{g}_0$. Put $U' = U \cap \mathfrak{g}_0'$ and $U_{\mathfrak{l}}' = U_{\mathfrak{l}} \cap \mathfrak{l}_0'$. Then we claim that $U' = U_\sigma + U_{\mathfrak{l}}'$. This is seen as follows. Let λ be an indeterminate and I the identity maping of $\mathfrak{g}$. Then it is obvious that

---

[1] We follow here the terminology of Chevalley [2]. The present computation is very similar to the one performed during the proof of Lemma 39 of [4(c)].

$$\det(\lambda I - \operatorname{ad} Z) = \det(\lambda I - \operatorname{ad} Z)_{\mathfrak{q}} \det(\lambda I - \operatorname{ad} Z)_{\mathfrak{z}} \qquad (Z \in \mathfrak{z}),$$

where the subscripts signify restrictions on the corresponding subspaces. Now suppose $Z \in U$ and $Z = H + Y$, where $H \in U_\sigma$ and $Y \in U_{\mathfrak{l}}$. Then it is evident that

$$\det(\lambda I - \operatorname{ad} Z)_{\mathfrak{z}} = \lambda^{l-1} \det(\lambda I - \operatorname{ad} Y)_{\mathfrak{l}},$$

and therefore $\det(\lambda I - \operatorname{ad} Z) = \lambda^{l-1} \det(\lambda I - \operatorname{ad} Z)_{\mathfrak{q}} \det(\lambda I - \operatorname{ad} Y)_{\mathfrak{l}}$. The coefficient of λ^l on the left side is $(-1)^r \eta(Z)$, where r is the number of roots in P. On the other hand, the constant term in $\det(\lambda I - \operatorname{ad} Z)_{\mathfrak{q}}$ is $(-1)^q \zeta(Z)$, where $q = \dim \mathfrak{q}$. Moreover, since $\mathfrak{l}$ is of rank 1, λ divides $\det(\lambda I - \operatorname{ad} Y)_{\mathfrak{l}}$, and the coefficient of λ in it is $-\frac{1}{2}\Omega(Y)$, where Ω is the Casimir polynomial of $\mathfrak{l}$ (see Section 6). This means that

$$(-1)^r \eta(Z) = \tfrac{1}{2}(-1)^{q+1} \zeta(Z) \Omega(Y).$$

Therefore, since ζ is never zero on U, $Z \in U'$ if and only if $Y \in \mathfrak{l}_0'$, and this proves that $U' = U_\sigma + U_{\mathfrak{l}}'$. In view of the above condition imposed on $U_{\mathfrak{l}}$, it follows (see Appendix, § 6) that $U_{\mathfrak{l}}'$ is connected or it has exactly three connected components according as $\mathfrak{l}_0$ is compact or not. Put $N' = N \cap \mathfrak{g}_0'$. Then $N' = \psi(V^* \times U')$, and therefore we get the following result.

LEMMA 2. *If $\alpha_0 \in P_-$ then $\mathfrak{l}_0$ is compact and $N \cap \mathfrak{g}_0'$ is connected. On the other hand, if $\alpha_0 \in Q_+ \cup P_0$, $\mathfrak{l}_0$ is not compact and $N \cap \mathfrak{g}_0'$ has exactly three connected components.*

From now on we shall assume that $\alpha_0 \in Q_+ \cup P_0$. Call an element $Z \in \mathfrak{l}_0'$ hyperbolic or elliptic according as $\Omega(Z)$ is positive or negative. Let $\mathfrak{l}_i$ $(i = 1, 2, 3)$ denote the three connected components of $\mathfrak{l}_0'$. We assume that Ω is positive on $\mathfrak{l}_1$ and negative on $\mathfrak{l}_2$ and $\mathfrak{l}_3$ (see Appendix, § 6). Put

$$H' = H_{\alpha_0}',\ X' = X_{\alpha_0},\ Y' = X_{-\alpha_0} \text{ if } \alpha_0 \in Q_+ \text{ and } H' = (-1)^{\frac{1}{2}}(X_{\alpha_0} - X_{-\alpha_0}),$$
$$X' = \tfrac{1}{2}\{X_{\alpha_0} + X_{-\alpha_0} + (-1)^{\frac{1}{2}} H_{\alpha_0}'\},\quad Y' = \tfrac{1}{2}\{X_{\alpha_0} + X_{-\alpha_0} - (-1)^{\frac{1}{2}} H_{\alpha_0}'\}$$

if $\alpha_0 \in P_0$. Then $\mathfrak{l}_0 = RH' + RX' + RY'$ and $[H', X'] = 2X'$ $[H', Y']$

$= -2Y'$, $[X', Y'] = H'$. Moreover H' is hyperbolic while $X' - Y'$ is elliptic. We shall suppose that $X' - Y' \in \mathfrak{l}_2$. Let $d\mu_\sigma$ and $d\mu_{\mathfrak{l}}$ denote the Euclidean measures on σ_0 and $\mathfrak{l}_0$, respectively. Every element in $\mathfrak{l}_0$ can be written in the form $tH' + xX' + yY'$ $(t, x, y \in R)$. We normalize $d\mu_{\mathfrak{l}}$ in such a way that[2] $d\mu_{\mathfrak{l}} = (2\pi)^{-1}dtdxdy$. Then since $\mathfrak{z}_0$ is the orthogonal sum of σ_0 and $\mathfrak{l}_0$, we can assume that $dZ = d\mu_\sigma d\mu_{\mathfrak{l}}$. Put

$$\mathfrak{a}_0 = \sigma_0 + RH' \quad \text{and} \quad \mathfrak{b}_0 = \sigma_0 + R(X' - Y').$$

Then $\mathfrak{a}_0$ and $\mathfrak{b}_0$ are Cartan subalgebras of $\mathfrak{z}_0$ (and also of $\mathfrak{g}_0$) which are invariant under θ. Let L be the analytic subgroup of G corresponding to $\mathfrak{l}_0$, and let K_1 be the connected component of 1 in $K \cap L$. Since $\mathfrak{l}_0 \cap \mathfrak{k}_0 = R(X' - Y')$, K_1 is the one-parameter subgroup corresponding to $X' - Y'$. Moreover K_1 is compact. For any $f \in C_c^\infty(\mathfrak{z}_0)$, put

$$\Phi_f(t, H_\sigma) = \int_{-\infty}^{\infty} \bar{f}(H_\sigma + tH' + xX')\,dx \qquad (t > 0),$$

$$\Psi_f(\phi, H_\sigma) = |\phi| \int_0^{\infty} \bar{f}(H_\sigma + \phi(e^tX' - e^{-t}Y'))\,(e^t - e^{-t})\,dt \quad (\phi \in R, \phi \neq 0)$$

for $H_\sigma \in \sigma_0$. Here $\bar{f}(Z) = \int_{K_1} f(k_1 z)\,dk_1$ $(Z \in \mathfrak{z}_0)$ and dk_1 is the normalized Haar measure on K_1 so that $\int_{K_1} dk_1 = 1$. Let R^+ and R^- denote the sets of all positive and negative real numbers, respectively, and put $R' = R^+ \cup R^-$. Also let $\mathfrak{a}_1$, $\mathfrak{b}_2$, $\mathfrak{b}_3$, respectively, denote the sets of all elements of the form $H_\sigma + tH'$, $H_\sigma + t(X' - Y')$ and $H_\sigma - t(X' - Y')$ $(t \in R^+)$. Put $\mathfrak{b}_0' = \mathfrak{b}_2 \cup \mathfrak{b}_3$. We can also regard Φ_f and Ψ_f as functions on $\mathfrak{a}_1$ and $\mathfrak{b}_0'$, respectively, as follows:

$$\Phi_f(H_\sigma + tH') = \Phi_f(t, H_\sigma), \qquad \Psi_f(H_\sigma + \phi(X' - Y')) = \Psi_f(\phi, H_\sigma)$$

$(H_\sigma \in \sigma_0, t \in R^+, \phi \in R')$. Let $\mathfrak{a}$, $\mathfrak{b}$ be the complexifications of $\mathfrak{a}_0$, $\mathfrak{b}_0$ in $\mathfrak{g}$. Consider the complex analytic subgroup L_c corresponding to $\mathfrak{l}$ in the (connected) complex adjoint group G_c of $\mathfrak{g}$. Define two elements $\nu_{\mathfrak{a}}$ and $\nu_{\mathfrak{b}}$ in L_c as follows. $\nu_{\mathfrak{a}} = 1$, $\nu_{\mathfrak{b}} = \exp\{(-1)^{\frac{1}{2}}(\pi/4)\,\mathrm{ad}(X_{\alpha_0} + X_{-\alpha_0})\}$ if[2] $\alpha_0 \in Q_+$ and $\nu_{\mathfrak{a}} = \exp\{-(-1)^{\frac{1}{2}}(\pi/4)\,\mathrm{ad}(X_{\alpha_0} + X_{-\alpha_0})\}$, $\nu_{\mathfrak{b}} = 1$ if $\alpha_0 \in P_0$. Then (see § 6) $H' = \nu_{\mathfrak{a}} H_{\alpha_0}'$, $(X' - Y') = (-1)^{\frac{1}{2}} \nu_{\mathfrak{b}} H_{\alpha_0}'$, and therefore $\nu_{\mathfrak{a}}\mathfrak{h} = \mathfrak{a}$, $\nu_{\mathfrak{b}}\mathfrak{h} = \mathfrak{b}$. For any root α of $\mathfrak{g}$ with respect to $\mathfrak{h}$, we define a root $\alpha_{\mathfrak{a}}$ with respect to $\mathfrak{a}$ by $\alpha_{\mathfrak{a}}(H) = \alpha(\nu_{\mathfrak{a}}^{-1}H)$ $(H \in \mathfrak{a})$. Similarly, define a root $\alpha_{\mathfrak{b}}$ with respect to $\mathfrak{b}$ by $\alpha_{\mathfrak{b}}(H) = \alpha(\nu_{\mathfrak{b}}^{-1}H)$ $(H \in \mathfrak{b})$. We shall say that $\alpha_{\mathfrak{a}}$ and $\alpha_{\mathfrak{b}}$ correspond to α

---

[2] Here π denotes, as usual, the smallest positive root of the equation $\sin t = 0$.

under $\nu_{\mathfrak{a}}$ and $\nu_{\mathfrak{b}}$, respectively. Put $\tau = (\alpha_0)_{\mathfrak{a}}$ and $\lambda = (\alpha_0)_{\mathfrak{b}}$. Then $\tau(H') = 2$ and $\lambda(X' - Y') = 2(-1)^{\frac{1}{2}}$. Let $P_{\mathfrak{a}}$ and $P_{\mathfrak{b}}$ be the sets of roots with respect to $\mathfrak{a}$ and $\mathfrak{b}$ corresponding to P under $\nu_{\mathfrak{a}}$ and $\nu_{\mathfrak{b}}$, respectively. Define the Euclidean measures $d\mu_{\mathfrak{a}}$, $d\mu_{\mathfrak{b}}$ on $\mathfrak{a}$, $\mathfrak{b}$ by $d\mu_{\mathfrak{a}} = d\mu_\sigma dt$, $d\mu_{\mathfrak{b}} = d\mu_\sigma d\phi$ corresponding to $H = H_\sigma + tH'$ and $\bar{H} = H_\sigma + \phi(X' - Y')$ $(H \in \mathfrak{a}_0;\ \bar{H} \in \mathfrak{b}_0;\ H_\sigma \in \sigma_0;\ t, \phi \in R)$. Put $\mathfrak{z}_i = \sigma_0 + \mathfrak{l}_i$ $(i = 1, 2, 3)$.

LEMMA 3. *For any* $f \in C_c^\infty(\mathfrak{z}_0)$ *define* Φ_f, Ψ_f *as above. Then* Φ_f *and* Ψ_f *lie in* $\mathcal{C}(\mathfrak{a}_1)$ *and* $\mathcal{C}(\mathfrak{b}_0')$, *respectively, and*

$$\int_{\mathfrak{z}_1} f(Z)\,dZ = \tfrac{1}{2}\int_{\mathfrak{a}_1} \tau\Phi_f d\mu_{\mathfrak{a}}, \qquad \int_{\mathfrak{z}_i} f(Z)\,dZ = \tfrac{1}{2}\int_{\mathfrak{b}_i} |\lambda|\,\Psi_f d\mu_{\mathfrak{b}} \quad (i = 2, 3).$$

Since σ is the center of $\mathfrak{z}$, it follows without difficulty that $\partial(p)\Phi_f = \Phi_{\partial(p)f}$, $\partial(p)\Psi_f = \Psi_{\partial(p)f}$ for $p \in S(\sigma)$ (see [4(d), § 2] for notation). Therefore since the carrier of f is compact, our statement follows from the work of the Appendix, especially Lemma 16.

Let Ξ' be the normalizer of σ_0 in G and Ξ_0 the analytic subgroup of G corresponding to $\mathfrak{z}_0$.

LEMMA 4. Ξ' *is also the normalizer of* $\mathfrak{z}_0$ *in* G *and every element of* Ξ' *leaves* $\mathfrak{l}_0$ *invariant. Moreover,* $\Xi' \supset \Xi \supset \Xi_0$ *and* Ξ_0 *is of finite index in* Ξ'.

Since σ_0 is the center of $\mathfrak{z}_0$ and $\mathfrak{z}_0$ the centralizer of σ_0 in $\mathfrak{g}_0$, it is obvious that Ξ' is also the normalizer of $\mathfrak{z}_0$ in G. Moreover, since $\mathfrak{l}_0$ is the derived algebra of $\mathfrak{z}_0$, $x\mathfrak{l}_0 = \mathfrak{l}_0$ for $x \in \Xi'$. Finally, since $\mathfrak{z}_0$ is the centralizer of H_0 in $\mathfrak{g}_0$, it is clear that $\Xi_0 \subset \Xi \subset \Xi'$. The finiteness of Ξ'/Ξ_0 is a consequence of Lemma 15 of the Appendix (Section 6).

We shall now show that if U is sufficiently small, $xU \cap U = \emptyset$ $(x \in G)$ unless $x \in \Xi$. This is done as follows. Since $S(\mathfrak{l}) \subset S(\mathfrak{g})$, we can regard Ω as a polynomial function on $\mathfrak{g}$. But then, since σ and $\mathfrak{l}$ are orthogonal, $\Omega(H + Z) = \Omega(Z)$ $(H \in \sigma, Z \in \mathfrak{l})$, and therefore $\Omega(H_0) = 0$. Choose a positive number δ. Then we may assume that U is so small that $|\Omega(Z)| < \delta^2 |\alpha(H_\sigma(Z))|^2$ $(Z \in U)$ for all $\alpha \neq \alpha_0$ in P. Here $H_\sigma(Z)$ denotes the orthogonal projection of Z in σ for any $Z \in \mathfrak{z}$. Since $[\sigma, \mathfrak{l}] = \{0\}$, it is clear that $H_\sigma(yZ) = H_\sigma(Z)$ $(y \in L_c, Z \in \mathfrak{z})$. Hence

$$\min_{\substack{\alpha \neq \alpha_0 \\ \alpha \in P}} |\alpha(H_\sigma(Z))| = \min_{\substack{\alpha \neq \tau \\ \alpha \in P_{\mathfrak{a}}}} |\alpha(H_\sigma(Z))| = \min_{\substack{\alpha \neq \lambda \\ \alpha \in P_{\mathfrak{b}}}} |\alpha(H_\sigma(Z))|.$$

Moreover, if $Z \in \mathfrak{a}$, $\Omega(Z) = 2\tau(Z)^2$ (see Section 6). Let $\tilde{U} = \bigcup_{y \in L} yU$. Then it follows that if $Z \in \bar{U} \cap \mathfrak{a}_0$

$$|\tau(Z)| < \delta\,|\alpha(H_\sigma(Z))| \text{ for all } \alpha \neq \tau \text{ in } P_{\mathfrak{a}}.$$

Similarly, if $Z \in \tilde{U} \cap \mathfrak{b}_0$, then $|\lambda(Z)| < \delta |\alpha(H_\sigma(Z))|$ for all $\alpha \neq \lambda$ in $P_{\mathfrak{b}}$. Now suppose δ is so small that $\delta \leqq \frac{1}{2}$ and

$$\delta |\alpha(H')| \leqq 1 \qquad (\alpha \in P_{\mathfrak{a}}), \qquad \delta |\beta(X' - Y')| \leqq 1 \qquad (\beta \in P_{\mathfrak{b}}).$$

Then since $Z = H_\sigma(Z) + \frac{1}{2}\tau(Z)H'$ for $Z \in \tilde{U} \cap \mathfrak{a}_0$, it follows that $\alpha(Z) = \alpha(H_\sigma(Z)) + \frac{1}{2}\tau(Z)\alpha(H')$ for $\alpha \in P_{\mathfrak{a}}$. Therefore if $\alpha \neq \tau$,

$$|\alpha(Z)| \geqq 2\delta |\alpha(Z)| \geqq 2\delta\{|\alpha(H_\sigma(Z))| - \tfrac{1}{2}|\tau(Z)|\,|\alpha(H')|\}$$
$$> (2 - \delta |\alpha(H')|)|\tau(Z)| \geqq |\tau(Z)|.$$

This proves that $|\alpha(Z)| > |\tau(Z)|$ for $Z \in \tilde{U} \cap \mathfrak{a}_0$ and $\alpha \neq \tau$ in $P_{\mathfrak{a}}$. Similarly, $|\alpha(Z)| > |\lambda(Z)|$ $(\alpha \in P_{\mathfrak{b}}, \alpha \neq \lambda)$ for $Z \in \tilde{U} \cap \mathfrak{b}_0$. Moreover, we have the following result.

LEMMA 5. *The two Cartan subalgebras* $\mathfrak{a}_0$ *and* $\mathfrak{b}_0$ *are not conjugate under* G.

Since $\theta(\sigma_0) = \sigma_0$, $H' \in \mathfrak{p}_0$ and $X' - Y' \in \mathfrak{k}_0$ (see [4(e), § 12]), it is clear that $\mathfrak{a}_0 \cap \mathfrak{k}_0 = \sigma_0 \cap \mathfrak{k}_0$ while $\mathfrak{b}_0 \cap \mathfrak{k}_0 = \sigma_0 \cap \mathfrak{k}_0 + R(X' - Y')$. Hence $l_-(\mathfrak{b}_0) = l_-(\mathfrak{a}_0) + 1$ in the notation of [4(e), § 8]. Therefore $\mathfrak{a}_0$ and $\mathfrak{b}_0$ cannot be conjugate.

Put $U_i = U \cap \mathfrak{z}_i$ $(i = 1, 2, 3)$.

COROLLARY. *Suppose* $Z_1 \in U_1$ *and* $Z_2 \in U_2 \cup U_3$. *Then* Z_1 *and* Z_2 *cannot be conjugate under* G.

For otherwise suppose $Z_2 = xZ_1$ $(x \in G)$. Since $U_1 \subset \sigma_0 + \mathfrak{l}_1$, we can select (see Section 6) $y_1 \in L$ such that $Z_1' = y_1 Z_1 \in \mathfrak{a}_1$. Similarly, we can choose $y_2 \in L$ such that $Z_2' = y_2 Z_2 \in \mathfrak{b}_0'$. Obviously Z_1, Z_2 are regular in $\mathfrak{g}_0$, and therefore the same holds for Z_1', Z_2'. Hence $\mathfrak{a}_0$ and $\mathfrak{b}_0$, respectively, are the centralizers of Z_1' and Z_2' in $\mathfrak{g}_0$. Moreover, $Z_2' = x'Z_1'$ $(x' = y_2 x y_1^{-1})$, and therefore $\mathfrak{b}_0 = x'\mathfrak{a}_0$. As this contradicts Lemma 5, the corollary follows.

Now suppose $xZ \in U$ for some $x \in G$ and $Z \in U$. First, let us assume that $Z \in U_1$. Then obviously xZ is regular in $\mathfrak{g}_0$, and so it follows from the Corollary to Lemma 5 that $xZ \in U_1$. Hence $y_1 Z$, $y_2 xZ$ are in $U_\sigma + R^+ H'$ for some $y_1, y_2 \in L$. Put $Z_1 = y_1 Z$ and $x_1 = y_2 x y_1^{-1}$. Then since $\mathfrak{a}_0$ is the centralizer in $\mathfrak{g}_0$ both of Z_1 and $x_1 Z_1$, we conclude that $x_1 \mathfrak{a}_0 = \mathfrak{a}_0$. Let $W_{\mathfrak{a}}$ be the Weyl group of $\mathfrak{g}$ with respect to $\mathfrak{a}$. Then x_1 defines an element $s \in W_{\mathfrak{a}}$. Put $s\tau = \tau'$ and $Z_2 = x_1 Z_1$. It is clear that $\tau'(Z_2) = \tau(Z_1)$. On the other hand, since $Z_1 \in \tilde{U} \cap \mathfrak{a}_0$, $|\tau(Z_1)| = \min_{\alpha \in P_{\mathfrak{a}}} |\alpha(Z_1)|$. Therefore $|\tau'(Z_2)| = \min_{\alpha \in P_{\mathfrak{a}}} |\alpha(Z_2)|$. But since Z_2 is also in $\tilde{U} \cap \mathfrak{a}_0$, we know that $|\tau(Z_2)|$

$< |\alpha(Z_2)|$ for any root $\alpha \neq \tau$ in $P_{\mathfrak{a}}$. Hence $\tau' = \pm\tau$. Now σ_0 is the set of all $H \in \mathfrak{a}_0$ where $\tau(H) = 0$. Therefore $x_1\sigma_0 = s\sigma_0 = \sigma_0$. Since L is contained in Ξ, this proves that $x \in \Xi'$.

Similarly, if $Z \in U_2 \cup U_3$, we can choose $y_1 \in L$ such that $Z_1 = y_1 Z \in U_\sigma + R'(X' - Y')$. Again it follows from the Corollary to Lemma 5 that $xZ \in U_2 \cup U_3$, and therefore $y_2 xZ \in U_\sigma + R'(X' - Y')$ for some $y_2 \in L$. Hence $x_1\mathfrak{b}_0 = \mathfrak{b}_0$ $(x_1 = y_2 x y_1^{-1})$ and the corresponding element s of the Weyl group $W_{\mathfrak{b}}$ (of $\mathfrak{g}$ with respect to $\mathfrak{b}$) maps λ into $\pm\lambda$, and therefore again $x \in \Xi'$.

Finally suppose Z is singular. For any $X \in \mathfrak{g}_0$, let $\mathfrak{n}_X$ denote the set of all $Y \in \mathfrak{g}_0$ such that $(\operatorname{ad} X)^q Y = 0$ for some integer $q \geqq 1$. We call $\mathfrak{n}_X$ the null space of X. It is obvious that if X is a singular element in U, $\mathfrak{n}_X = \mathfrak{z}_0$. Hence $\mathfrak{z}_0$ is the null space of both Z and xZ, and therefore $x\mathfrak{z}_0 = \mathfrak{z}_0$. In view of Lemma 4 this implies again that $x \in \Xi'$.

Now from Lemma 4, we can select a finite number of elements $u_0 = 1, u_1, \cdots, u_M \in \Xi'$ such that the cosets $u_i\Xi_0$ $(0 \leqq i \leqq M)$ are distinct and their union is Ξ'. Suppose $u_i \in \Xi$ for $0 \leqq i \leqq m$ and $u_i \notin \Xi$ for $m < i \leqq M$. Then $u_i H_0 \neq H_0$ $(m < i \leqq M)$, and we may assume that U_σ is so small that $U_\sigma \cap u_i U_\sigma = \emptyset$ $(m < i \leqq M)$. Select i such that $x \in u_i\Xi_0$. Then we claim that $i \leqq m$. For otherwise, suppose $i > m$. Since $U = U_\sigma + U_{\mathfrak{l}}$, it follows that $xU = xU_\sigma + xU_{\mathfrak{l}}$. On the other hand, from Lemma 4, xU_σ and $xU_{\mathfrak{l}}$ are contained in σ_0 and $\mathfrak{l}_0$, respectively, and since σ is the center of $\mathfrak{z}$, $xU_\sigma = u_i U_\sigma$, and therefore $U_\sigma \cap xU_\sigma = \emptyset$. But obviously, this implies that $U \cap xU = \emptyset$, and we get a contradiction with our assumption that $xZ \in U \cap xU$. Hence $i \leqq m$ and therefore $x \in \Xi$.

Put $\bar{U}_\sigma = \bigcap_{1 \leqq i \leqq m} u_i U_\sigma$, $\bar{U}_{\mathfrak{l}} = \bigcup_{\xi \in \Xi} \xi U_{\mathfrak{l}}$ and $\bar{U} = \bar{U}_\sigma + \bar{U}_{\mathfrak{l}}$. Since U_σ is convex, the same holds for $\bar{U}_\sigma$. Moreover, in view of its definition, Ω is invariant under any automorphism of $\mathfrak{l}$. Hence if $Z \in \bar{U}_{\mathfrak{l}}$, it is clear that $|\Omega(Z)| < \delta^2 |\alpha(H_\sigma(Z))|^2$ for all roots $\alpha \neq \alpha_0$ in P. Therefore it follows from the above proof that $x\bar{U} \cap \bar{U} = \emptyset$ $(x \in G)$ unless $x \in \Xi$.

LEMMA 6. *It is possible to select U in Lemma 1 so that it satisfies the following two further conditions.*

(1) $\xi U = U$ $(\xi \in \Xi)$,

(2) $U \cap xU = \emptyset$ *for any* $x \in G$ *which is not in* Ξ.

As we have already seen, $\bar{U}$ satisfies the above two conditions. The univalence of the mapping $(x^*, Z) \to \phi(x^*)Z$ of $V^* \times \bar{U}$ into $\mathfrak{g}_0$ is an immediate consequence of the second condition. Since the earlier conditions imposed on U (see p. 656) are obviously fulfilled by $\bar{U}$, the statement of the lemma follows.

Let A and B be the Cartan subgroups of G corresponding to $\mathfrak{a}_0$ and $\mathfrak{b}_0$, respectively. Since L is a normal subgroup of Ξ' (see Lemma 4), AL and BL are subgroups of Ξ and $AL = LA$, $BL = LB$. Let $[\Xi : LB]$ denote the index of LB in Ξ.

LEMMA 7. *$\Xi = LA$ and $[\Xi : LB] \leqq 2$. Let s_λ denote the Weyl reflexion in $W_{\mathfrak{b}}$ corresponding to the root $\lambda \in P_{\mathfrak{b}}$. Then $[\Xi : LB] = 2$ if and only if there exists an element $\xi \in \Xi$ which coincides with s_λ on $\mathfrak{b}$.*

Let x be any element in Ξ. Then $x\mathfrak{l}_0 = \mathfrak{l}_0$ from Lemma 4, and therefore $\Omega(xH') = \Omega(H')$, $\Omega(x(X' - Y')) = \Omega(X' - Y')$. This shows that $xH' \in \mathfrak{l}_1$ and $x(X' - Y') \in \mathfrak{l}_2 \cup \mathfrak{l}_3$. Hence we can select $y_1, y_2 \in L$ such that $y_1^{-1}xH' \in R^{-}H'$ and $y_2^{-1}x(X' - Y') \in R'(X' - Y')$. But since $\operatorname{sp}(\operatorname{ad}(zX))^2 = \operatorname{sp}(\operatorname{ad} X)^2$ $(z \in G, X \in \mathfrak{g})$ this implies that $y_2^{-1}xH' = H'$ and $y_2^{-1}x(X' - Y') = \pm(X' - Y')$. Now if t is sufficiently small and positive, $H_0 + tH'$ is nonsingular and so its centralizer in G is A (see [4(c), Lemma 3]). Hence $y_1^{-1}x \in A$, and so $x \in LA$. This proves that $\Xi = LA$. On the other hand, choose, if possible, an element $\xi \in \Xi$ such that $\xi(X' - Y') = -(X' - Y')$. In case $y_2^{-1}x(X' - Y') = X' - Y'$, the above argument applied to $H_0 + t(X' - Y')$ $(t \in R')$ shows that $x \in LB$. So now suppose $y_2^{-1}x(X' - Y') = -(X' - Y')$. Then $\xi^{-1}y_2^{-1}x(X' - Y') = (X' - Y')$, and therefore $\xi^{-1}y_2^{-1}x \in B$. This proves that $x \in L\xi B = \xi LB$ in this case. Hence $[\Xi : LB] \leqq 2$. Moreover, it is obvious that $[\Xi : LB] = 1$ if ξ does not exist. So let us assume that ξ exists. We claim $\xi \notin LB$. For otherwise, $\xi = yb$ $(y \in L, b \in B)$, and therefore $y(X' - Y') = \xi(X' - Y') = -(X' - Y')$. But this is impossible (see Section 6), and therefore $[\Xi : LB] = 2$ in this case. Since $\xi\sigma = \sigma$, it is clear that $\xi\mathfrak{b} = \mathfrak{b}$. Let s be the element of $W_{\mathfrak{b}}$ corresponding to ξ. Then

$$\begin{aligned} s(H_0 + t(X' - Y')) &= \xi(H_0 + t(X' - Y')) \\ &= H_0 - t(X' - Y') = s_\lambda(H_0 + t(X' - Y')) \quad (t \in R). \end{aligned}$$

But if t is suitably chosen, $H_0 + t(X' - Y')$ is regular in $\mathfrak{g}_0$. Then since $s^{-1}s_\lambda$ leaves it fixed, we can conclude (see [4(c), Lemma 4]) that $s = s_\lambda$. This completes the proof of the lemma.

Now select U once for all according to Lemma 6.

COROLLARY. *Let x be an element in G such that $x(\mathfrak{a}_1 \cap U)$ meets $\mathfrak{a}_1 \cap U$. Then $x \in A$. Similarly, if $y(\mathfrak{b}_i \cap U)$ meets $\mathfrak{b}_i \cap U$ $(y \in G, i = 2, 3)$, then $y \in B$.*

Select $H_1 \in \mathfrak{a}_1 \cap U$ such that $xH_1 \in \mathfrak{a}_1 \cap U$. Then since $\mathfrak{a}_0$ is the centralizer in $\mathfrak{g}_0$ of both H_1 and $H_2 = xH_1$, $\mathfrak{a}_0 = x\mathfrak{a}_0$. Hence x defines an element $s \in W_{\mathfrak{a}}$. But $x\sigma = \sigma$, since $x \in \Xi$ from Lemma 6. Therefore it is clear that $s\tau = \pm \tau$. But $\tau(s^{-1}H_2) = \tau(H_1) > 0$ and $H_2 \in \mathfrak{a}_1$. So we conclude that $s\tau = \tau$, and therefore $sH' = H'$. This proves that $x(H_0 + tH') = H_0 + tH'$ $(t \in R)$, and therefore from [4(c), Lemma 3] $x \in A$. The proof in the other case is quite similar.

Define $N = \psi(V^* \times U)$ as in Lemma 1, and put $U_i = U \cap \mathfrak{z}_i$, $N_i = \psi(V^* \times U_i)$ $(i = 1, 2, 3)$. Moreover, let $\mathfrak{b}^+ = \mathfrak{b}_2$, $\mathfrak{b}^- = \mathfrak{b}_3$, $N^+ = N_2$, $N^- = N_3$ if $[\Xi : LB] = 1$ and $\mathfrak{b}^+ = \mathfrak{b}^- = \mathfrak{b}_2 \cup \mathfrak{b}_3$, $N^+ = N^- = N_2 \cup N_3$ if $[\Xi : LB] = 2$. Let p be any polynomial in $S(\mathfrak{g})$ which is invariant under L. Then we denote by $p_{\mathfrak{a}}$ and $p_{\mathfrak{b}}$ its restrictions on $\mathfrak{a}$ and $\mathfrak{b}$, respectively. The following lemma contains the main result of this section.

LEMMA 8. *For any $\gamma \in C_c^\infty(U)$, define $f_\gamma \in C_c^\infty(N)$ as in Lemma* 1. *Then*

$$\int_{N_1} p\partial(q) f_\gamma \, dX = \tfrac{1}{2} \int_{\mathfrak{a}_1} \tau p_{\mathfrak{a}} \, |\, \zeta_{\mathfrak{a}} \,|^{\frac{1}{2}} \partial(q_{\mathfrak{a}}) \Phi_{|\zeta|^{\frac{1}{2}}\gamma} \, d\mu_{\mathfrak{a}},$$

$$\int_{N^\pm} p\partial(q) f_\gamma \, dX = \tfrac{1}{2} \int_{\mathfrak{b}^\pm} |\, \lambda \,|\, p_{\mathfrak{b}} \, |\, \zeta_{\mathfrak{b}} \,|^{\frac{1}{2}} \partial(q_{\mathfrak{b}}) \Psi_{|\zeta|^{\frac{1}{2}}\gamma} \, d\mu_{\mathfrak{b}}$$

for $p, q \in I(\mathfrak{g})$ and $\gamma \in C_c^\infty(U)$.

If U_σ is the orthogonal projection of U in σ_0, $U \cap \mathfrak{a}_1 \subset U_\sigma + R_1 H' \subset \mathfrak{a}_0 \cap \mathfrak{g}_0'$ where R_1 is an open interval in R^+. Therefore, since U_σ is connected, $U \cap \mathfrak{a}_1$ is contained in a connected component of $\mathfrak{a}_0 \cap \mathfrak{g}_0'$. Put $\pi_{\mathfrak{a}} = \prod_{\alpha \in P_{\mathfrak{a}}} \alpha$. Then $\pi_{\mathfrak{a}}^2$ takes only real values on $\mathfrak{a}_0$, and so we can select a complex number ϵ such that $\epsilon^4 = 1$ and $\epsilon\pi_{\mathfrak{a}}$ is everywhere positive on $U \cap \mathfrak{a}_1$. Since $U_1 \subset U_\sigma + \mathfrak{l}_1$, it is obvious that $N_1 \subset \bigcup_{x \in G} x(\mathfrak{a}_1 \cap U)$. We claim $N_1 = N \cap \bigcup_{x \in G} x(\mathfrak{a}_1 \cap U)$. For suppose $zH \in N$ for some $z \in G$ and $H \in \mathfrak{a}_1 \cap U$. Then $zH = \phi(x^*)Z$ for some $x^* \in V^*$ and $Z \in U$. It follows from the Corollary to Lemma 5 that $Z \in U_1$ and therefore $Z = yH_1$ $(y \in L, H_1 \in \mathfrak{a}_1 \cap U)$. But then we conclude from Lemma 6 that $z^{-1}\phi(x^*)y \in \Xi$, and therefore $z \in \phi(x^*)\Xi$. Since $\Xi H \subset U_1$ (by the Corollary to Lemma 5), it follows that $zH \in \phi(x^*)U_1 \subset N_1$, and this proves our assertion. *Moreover, the above argument shows that if $zH \in N$ $(z \in G, H \in \mathfrak{a}_1 \cap U)$, then $z^* \in V^*$.* We shall need this fact presently.

Put $\bar{G} = G/A$ and define $\bar{x}H = xH$ $(x \in G, H \in \mathfrak{a}_0)$, where $x \to \bar{x}$ is the natural mapping of G onto $\bar{G}$. Then in view of the above result and the

Corollary to Lemma 7, we can normalize the invariant measure $d\bar{x}$ on $\bar{G}$ in such a way (see [4(a), p. 501]) that

$$\int_{N_1} g(X)\,dX = \int_{\mathfrak{a}_1\cap U} (\epsilon\pi_{\mathfrak{a}}(H))^2 d\mu_{\mathfrak{a}} \int_{\bar{G}} g(\bar{x}H)\,d\bar{x} \qquad (g\in C_c(N_1)).$$

Put $\bar{\Xi}=\Xi/A$ and let $d\bar{\xi}$ denote the invariant measure on $\bar{\Xi}$. Then it is clear that if $d\bar{\xi}$ is suitably normalized,

$$\int_{\bar{G}} g(\bar{x}H)\,d\bar{x} = \int_{G^*} dx^* \int_{\bar{\Xi}} g(x(\bar{\xi}H))\,d\bar{\xi} \qquad (g\in C_c^\infty(\mathfrak{g}_0), H\in\mathfrak{a}_0\cap\mathfrak{g}_0').$$

Now put $\psi_g(H)=\pi_{\mathfrak{a}}(H)\int_{\bar{G}} g(\bar{x}H)\,d\bar{x}$ $(H\in\mathfrak{a}_0\cap\mathfrak{g}_0')$ for $g\in C_c^\infty(\mathfrak{g}_0)$. (It follows from Theorem 3 of [4(e)] that the above integral is convergent.) Then if $g=f_\gamma$ $(\gamma\in C_c^\infty(U))$,

$$\psi_{f_\gamma}(H)=\pi_{\mathfrak{a}}(H)\int_{G^*} dx^* \int_{\bar{G}} f_\gamma(x(\bar{\xi}H))\,d\bar{\xi} \qquad (H\in\mathfrak{a}_1\cap U).$$

We have seen above that if $zH\in N$ for some $z\in G$ and $H\in\mathfrak{a}_1\cap U$, then $z^*\in V^*$. Therefore

$$\psi_{f_\gamma}(H)=\pi_{\mathfrak{a}}(H)\int_{V^*} dx^* \int_{\bar{G}} f_\gamma(\phi(x^*)(\bar{\xi}H))\,d\bar{\xi} \qquad (H\in\mathfrak{a}_1\cap U).$$

But $f_\gamma(\phi(x^*)Z)=a_0(x^*)\gamma(Z)$ $(x^*\in V^*, Z\in U)$ from the definition of f_γ. Therefore, since U is invariant under Ξ, we get

$$\psi_{f_\gamma}(H)=\pi_{\mathfrak{a}}(H)\int_{V^*} a_0(x^*)\,dx^* \int_{\bar{\Xi}} \gamma(\bar{\xi}H)\,d\bar{\xi}$$
$$=\pi_{\mathfrak{a}}(H)\int_{\bar{\Xi}} \gamma(\bar{\xi}H)\,d\bar{\xi} \qquad (H\in\mathfrak{a}_1\cap U).$$

Moreover, since $\Xi=LA$ it is obvious (see Section 6) that

$$\tau(H)\int_{\bar{\Xi}} \gamma(\bar{\xi}H)\,d\bar{\xi}=c\Phi_\gamma(H) \qquad (H\in\mathfrak{a}_1),$$

where c is a positive number independent of H or γ. Therefore

$$\psi_{f_\gamma}(H)=c\pi_{\mathfrak{a}}'(H)\Phi_\gamma(H) \qquad (\gamma\in C_c^\infty(U), H\in\mathfrak{a}_1\cap U),$$

where $\pi_{\mathfrak{a}}'$ is the product of all roots $\alpha\neq\tau$ in $P_{\mathfrak{a}}$. On the other hand, ζ is invariant under L and since τ is everywhere positive on $\mathfrak{a}_1$, it is clear that $|\zeta_{\mathfrak{a}}|^{\frac{1}{2}}=\epsilon\pi_{\mathfrak{a}}'$ on $\mathfrak{a}_1\cap U$. Hence $\psi_{f_\gamma}=c\epsilon^{-1}\Phi_{|\zeta|^{\frac{1}{2}}\gamma}$ on $\mathfrak{a}_1\cap U$. Now suppose $p, q\in I(\mathfrak{g})$. Then

$$\int_{N_1} p(X) f_\gamma(X;\partial(q))\,dX = \int_{\mathfrak{a}_1\cap U} (\epsilon\pi_{\mathfrak{a}}(H))^2 p(H)\,d\mu_{\mathfrak{a}} \int_{\bar{G}} f_\gamma(\bar{x}H;\partial(q))\,d\bar{x}$$

$$= \epsilon^2 \int_{\mathfrak{a}_1\cap U} \pi_{\mathfrak{a}}(H) p(H) \psi_{f\gamma}(H;\partial(q_{\mathfrak{a}}))\,d\mu_{\mathfrak{a}}$$

from Theorem 3 of [4(e)]. But

$$\epsilon^2\pi_{\mathfrak{a}}\partial(q_{\mathfrak{a}})\psi_{f\gamma} = c\epsilon\pi_{\mathfrak{a}}'\tau\partial(q_{\mathfrak{a}})(\Phi_{|\zeta|^{\frac{1}{2}}\gamma}) = c\,|\,\zeta_{\mathfrak{a}}\,|^{\frac{1}{2}}\tau\partial(q_{\mathfrak{a}})(\Phi_{|\zeta|^{\frac{1}{2}}\gamma})$$

on $\mathfrak{a}_1\cap U$. Therefore since $\Phi_{|\zeta|^{\frac{1}{2}}\gamma}$ is zero on $\mathfrak{a}_1$ outside $\mathfrak{a}_1\cap U$, it follows that

$$\int_{N_1} p(X) f_\gamma(X;\partial(q))\,dX = c\int_{\mathfrak{a}_1} |\,\zeta_{\mathfrak{a}}\,|^{\frac{1}{2}}\tau p_{\mathfrak{a}}\partial(q_{\mathfrak{a}})\Phi_{|\zeta|^{\frac{1}{2}}\gamma}\,d\mu_{\mathfrak{a}}.$$

In order to determine c, we put $p=q=1$. Then

$$\int_{N_1} f_\gamma\,dX = c\int_{\mathfrak{a}_1} |\,\zeta_{\mathfrak{a}}\,|^{\frac{1}{2}}\tau\Phi_{|\zeta|^{\frac{1}{2}}\gamma}\,d\mu_{\mathfrak{a}} = c\int_{\mathfrak{a}_1}\tau\Phi_{|\zeta|\gamma}\,d\mu_{\mathfrak{a}} = 2c\int_{U_1} |\,\zeta\,|\,\gamma\,dZ$$

from Lemma 3. Therefore we conclude from Lemma 1 that $c=\frac{1}{2}$.

Now we come to the second formula. Since $U_i \subset U_\sigma + \mathfrak{l}_i$ $(i=2,3)$, we prove as before that $N_i \subset \bigcup_{x\in G} x(\mathfrak{b}_i\cap U)$. Moreover, by the same argument as used above, we show that $N_2\cup N_3 = N\cap(\bigcup_{x\in G} x(\mathfrak{b}_0'\cap U))$. Now first suppose $[\Xi : LB]=1$. Then no point in N_2 can be conjugate (under G) to a point in N_3. For otherwise, we could choose $H_i\in\mathfrak{b}_i\cap U$ $(i=2,3)$ and $x\in G$ such that $xH_2=H_3$. But as we have seen during the proof of Lemma 7, this implies that x coincides with s_λ on $\mathfrak{b}$, which is impossible since $[\Xi : LB]=1$. Hence $N_i\cap(\bigcup_{x\in G} x(\mathfrak{b}_j\cap U))$ is empty if $i=2$, $j=3$ or $i=3$, $j=2$. This shows that $N_i = N\cap\bigcup_{x\in G} x(\mathfrak{b}_i\cap U)$ $(i=2,3)$ in this case, and the proof of the second formula now proceeds in the same way as that of the first.

So let us now assume that $[\Xi : LB]=2$ and select an element $z\in\Xi$ which coincides with s_λ on $\mathfrak{b}$. Then $z\mathfrak{b}_2=\mathfrak{b}_3$ and therefore $N_2\cup N_3 = N\cap(\bigcup_{x\in G} x(\mathfrak{b}_2\cap U))$. Define $\pi_{\mathfrak{b}} = \prod_{\alpha\in P_{\mathfrak{b}}}\alpha$ and choose, as before, a complex number ϵ such that $\epsilon^4=1$ and $\epsilon\pi_{\mathfrak{b}}^2$ is everywhere positive on $U\cap\mathfrak{b}_2$. We use our earlier notation except that now $\bar{G}=G/B$, $\bar{\Xi}=\Xi/B$ and

$$\psi_g(H) = \pi_{\mathfrak{b}}(H)\int_{\bar{G}} g(\bar{x}H)\,d\bar{x} \qquad (H\in\mathfrak{b}_0\cap\mathfrak{g}_0',\ g\in C_c^\infty(\mathfrak{g}_0)).$$

Then again

$$\psi_{f\gamma}(H) = \pi_{\mathfrak{b}}(H)\int_{\bar{\Xi}} \gamma(\bar{\xi}H)\,d\bar{\xi} \qquad (H\in\mathfrak{b}_2\cap\mathfrak{g}_0',\ \gamma\in C_c^\infty(U)).$$

Let $\bar{L}=(LB)/B$. Then since $\Xi=LB\cup(LB)z$, it follows that

$$\int_{\bar{\Xi}}\gamma(\bar{\xi}H)\,d\bar{\xi}=\int_{\bar{L}}\gamma(\bar{\xi}H)\,d\bar{\xi}+\int_{\bar{L}}\gamma(\bar{\xi}(s_\lambda H))\,d\bar{\xi}\qquad(H\in\mathfrak{b}_2).$$

Moreover it is clear (see Section 6) that there exists a positive number c such that

$$|\lambda(H)|\int_{\bar{L}}\gamma(\bar{\xi}H)\,d\bar{\xi}=c\Psi_\gamma(H)\qquad(H\in\mathfrak{b}_2\cup\mathfrak{b}_3,\gamma\in C_c^\infty(U)).$$

For any function g on $\mathfrak{b}_2\cup\mathfrak{b}_3$, let $g^{s\lambda}$ denote the function $H\rightarrow g(s_\lambda H)$ $(H\in\mathfrak{b}_2\cup\mathfrak{b}_3)$. Then since $\epsilon\pi_{\mathfrak{b}}=|\pi_{\mathfrak{b}}|=|\zeta_{\mathfrak{b}}|^{\frac{1}{2}}|\lambda|$ on $\mathfrak{b}_2\cap U$, we conclude that

$$\psi_{f\gamma}=c\epsilon^{-1}\{\Psi_{|\zeta|^{\frac{1}{2}}\gamma}+(\Psi_{|\zeta|^{\frac{1}{2}}\gamma})^{s\lambda}\}$$

on $\mathfrak{b}_2\cap U$. Now suppose $p,q\in I(\mathfrak{g})$. Then since

$$N^+=N_2\cup N_3=N\cap\bigcup_{x\in G}x(\mathfrak{b}_2\cap U),$$

it follows that

$$\int_{N^+}p(X)f_\gamma(X;\partial(q))\,dX=\int_{\mathfrak{b}_2\cap U}(\epsilon\pi_{\mathfrak{b}}(H))^2p(H)\,d\mu_{\mathfrak{b}}\int_{\bar{G}}f_\gamma(\bar{x}H;\partial(q))\,d\bar{x}$$

$=\epsilon^2\int_{\mathfrak{b}_2\cap U}\pi_{\mathfrak{b}}(H)p(H)\psi_{f\gamma}(H;\partial(q_{\mathfrak{b}}))\,d\mu_{\mathfrak{b}}$ as before. Furthermore,

$$\epsilon^2\pi_{\mathfrak{b}}\partial(q_{\mathfrak{b}})\psi_{f\gamma}=c\,|\zeta_{\mathfrak{b}}|^{\frac{1}{2}}|\lambda|\,\partial(q_{\mathfrak{b}})\{\Psi_{|\zeta|^{\frac{1}{2}}\gamma}+(\Psi_{|\zeta|^{\frac{1}{2}}\gamma})^{s\lambda}\}$$

on $\mathfrak{b}_2\cap U$. Therefore, since $\mathfrak{b}^+=\mathfrak{b}_2\cup\mathfrak{b}_3$, it is clear that

$$\int_{N^+}p\partial(q)f_\gamma\,dX=c\int_{\mathfrak{b}^+}|\zeta_{\mathfrak{b}}|^{\frac{1}{2}}|\lambda|\,p_{\mathfrak{b}}\partial(q_{\mathfrak{b}})\Psi_{|\zeta|^{\frac{1}{2}}\gamma}\,d\mu_{\mathfrak{b}}.$$

In order to determine c, we again put $p=q=1$. Then

$$\int_{N^+}f_\gamma\,dX=c\int_{\mathfrak{b}^+}|\lambda|\,\Psi_{|\zeta|\gamma}\,d\mu_{\mathfrak{b}}=2c\int_{U_2\cup U_3}|\zeta|\,\gamma\,dZ$$

from Lemma 3. Therefore $c=\frac{1}{2}$ from Lemma 1. This completes the proof of Lemma 8.

Define the polynomial $\eta\in I(\mathfrak{g})$ as in [4(e), § 6] and put $\epsilon_{\mathfrak{a}}=|\pi_{\mathfrak{a}}|\pi_{\mathfrak{a}}^{-1}$, $\epsilon_{\mathfrak{b}}=|\pi_{\mathfrak{b}}|\pi_{\mathfrak{b}}^{-1}$ on $\mathfrak{a}_1\cap U$ and $\mathfrak{b}_0'\cap U$, respectively. Then as we have seen above, $\epsilon_{\mathfrak{a}}$ and $\epsilon_{\mathfrak{b}}$ are constant on $\mathfrak{a}_1\cap U$ and $\mathfrak{b}_i\cap U$ $(i=2,3)$, respectively. Moreover since $\pi_{\mathfrak{b}}^{s\lambda}=-\pi_{\mathfrak{b}}$, it is clear that $\epsilon_{\mathfrak{b}}(H_2)=-\epsilon_{\mathfrak{b}}(H_3)$ if $H_i\in\mathfrak{b}_i\cap U$ $(i=2,3)$.

COROLLARY. *Let k be any integer $\geqq 0$. Then for any $\xi \in I(\mathfrak{g})$,*

$$\int_{N_1} \eta^k \partial(\eta^k \xi) \bar{f}_\gamma \, dX = \tfrac{1}{2} \int_{\mathfrak{a}_1} \epsilon_{\mathfrak{a}} \pi_{\mathfrak{a}}^{2k+1} \partial(\pi_{\mathfrak{a}}^{2k} \xi_{\mathfrak{a}}) \Phi_{|\zeta|^{\frac{1}{2}}\gamma} d\mu_{\mathfrak{a}},$$

$$\int_{N^{\pm}} \eta^k \partial(\eta^k \xi) \bar{f}_\gamma \, dX = \tfrac{1}{2} \int_{\mathfrak{b}^{\pm}} \epsilon_{\mathfrak{b}} \pi_{\mathfrak{b}}^{2k+1} \partial(\pi_{\mathfrak{b}}^{2k} \xi_{\mathfrak{b}}) \Psi_{|\zeta|^{\frac{1}{2}}\gamma} d\mu_{\mathfrak{b}}$$

for $\gamma \in C_c^\infty(U)$.

This follows immediately from Lemma 8 if we observe that $\eta_{\mathfrak{a}} = \pi_{\mathfrak{a}}^2$, $\eta_{\mathfrak{b}} = \pi_{\mathfrak{b}}^2$ and $\tau |\zeta_{\mathfrak{a}}|^{\frac{1}{2}} = |\pi_{\mathfrak{a}}| = \epsilon_{\mathfrak{a}} \pi_{\mathfrak{a}}$, $|\lambda| |\zeta_{\mathfrak{b}}|^{\frac{1}{2}} = |\pi_{\mathfrak{b}}| = \epsilon_{\mathfrak{b}} \pi_{\mathfrak{b}}$ on $\mathfrak{a}_1 \cap U$ and $\mathfrak{b}_0' \cap U$, respectively.

3. Proof of Theorem 1.

Since $\mathfrak{h} = \sigma + CH_{\alpha_0}$, it is clear that every polynomial in $S(\mathfrak{h})$ can be written uniquely in the form $p = \sum_{k \geqq 0} p_k \alpha_0^k$ where $p_k \in S(\sigma)$. Let s_0 denote the Weyl reflexion in $\mathfrak{h}$ corresponding to α_0. Then since H_{α_0} is orthogonal to σ, it is obvious that $p_k^{s_0} = p_k$ and $s_0 \alpha_0 = -\alpha_0$. Therefore if $p^{s_0} = p$, we can conclude that $p_k = 0$ if k is odd. Now let ξ be a homogeneous element in $I(\mathfrak{g})$ of positive degree and r an integer $\geqq 0$. Then if $\bar{\xi}$ is the restriction of ξ on $\mathfrak{h}$, it follows that (see [4(d), Lemma 9]) that

$$\bar{\xi} \pi^{2r} = \sum_{k \geqq 0} \alpha_0^{2r+2k} q_k,$$

where $q_k \in S(\sigma)$. Similarly,

$$\pi^{2r+1} = \sum_{m \geqq 0} \alpha_0^{2r+1+2m} q_m',$$

where again $q_m' \in S(\sigma)$. Put

$$p_k = \sum_{m \geqq 0} \langle \alpha_0^{2r+1+2m}, \alpha_0^{2r+1+2m} \rangle \partial(q_{m+1+k}) q_m' \qquad (k \geqq 0)$$

in the notation of [4(d), § 2]. Let $d^0(p)$ denote the degree of any polynomial $p \in S(\mathfrak{g})$. Then it is obvious that q_k and q_m' are homogeneous and

$$d^0(q_k) = d^0(\xi) + 2r d^0(\pi) - (2r + 2k),$$

$$d^0(q_m') = (2r+1) d^0(\pi) - (2r + 1 + 2m).$$

Therefore p_k is also homogeneous and

$$d^0(p_k) = d^0(\pi) - d^0(\xi) + 2k + 1 \qquad (k \geqq 0).$$

LEMMA 9. *For any given integer $r \geqq 0$, we can choose a homogeneous element $\xi \in I(\mathfrak{g})$ of positive degree such that the corresponding polynomial $p_k \neq 0$ for some k.*

Put $\epsilon = 1$ or $(-1)^{\frac{1}{2}}$ according as α_0 lies in Q_+ or in P_0. Then $\alpha^* = \epsilon\alpha_0$ takes only real values on $\mathfrak{h}_0$. Let $\mathfrak{h}_+$ denote the set of all $H \in \mathfrak{h}_0$ where $\alpha^*(H) > 0$. Similarly, let $\mathfrak{h}_-$ be the set of those $H \in \mathfrak{h}_0$ where $\alpha^*(H) < 0$. We call $\mathfrak{h}_+$ and $\mathfrak{h}_-$, respectively, the upper and lower halves of $\mathfrak{h}_0$.

Let $d\mu$ denote the Euclidean measure on $\mathfrak{h}_0$ and $\mathcal{E}$ the distribution on $\mathfrak{h}_0$ given by

$$\mathcal{E}(g) = \int_{\mathfrak{h}_+} g \, d\mu \qquad (g \in C_c^\infty(\mathfrak{h}_0)).$$

Put $\mathcal{E}_r = \partial(\pi^{2r})(\pi^{2r+1}\mathcal{E})$. We shall first prove the following result.

LEMMA 10. *There exists a homogenous element* $\bar{\xi} \in I(\mathfrak{h})$ *of positive degree such that* H_0 *lies in the carrier of* $\partial(\bar{\xi})\mathcal{E}_r$.

Let $\square$ denote the polynomial function on $\mathfrak{h}$ defined by $\square(H) = -B(H, \theta(H))$ $(H \in \mathfrak{h})$. Let W be the Weyl group of $\mathfrak{g}$ with respect to $\mathfrak{h}$, and consider the polynomial

$$\prod_{s \in W} (t - \square^s) = t^w + q_1 t^{w-1} + \cdots + q_w \qquad (q_i \in S(\mathfrak{h}))$$

in the indeterminate t with coefficients in $S(\mathfrak{h})$. It is obvious that q_i $(1 \leqq i \leqq w)$ are homogeneous elements in $I(\mathfrak{h})$ of positive degree. Replacing t by $\square$ we get,

$$\square^w + \square^{w-1} q_1 + \cdots + q_w = \prod_{s \in W} (\square - \square^s) = 0.$$

Now if our assertion is false, we can choose an open connected neighborhood V of H_0 in $\mathfrak{h}_0$ such that $\partial(q_i)\mathcal{E}_r = 0$ on V $(1 \leqq i \leqq w)$. Therefore since

$$\partial(\square^w) + \partial(\square^{w-1})\partial(q_1) + \cdots + \partial(q_w) = 0,$$

we conclude that $\partial(\square^w)\mathcal{E}_r = 0$ on V. But $\square$ is obviously a positive-definite quadratic form in $\mathfrak{h}_0$, and therefore this differential equation is of the *elliptic type* (see Garding [3]). Hence it follows (see [7, p. 136] and [6]) that $\mathcal{E}_r$ must coincide on V with an analytic function. But $\mathcal{E} = 0$ on $\mathfrak{h}_-$, and therefore $\mathcal{E}_r = 0$ on $V \cap \mathfrak{h}_-$. Moreover, $V \cap \mathfrak{h}_-$ is open and not empty since $\alpha_0(H_0) = 0$. Therefore we conclude that $\mathcal{E}_r = 0$ on V. On the other hand, $V \cap \mathfrak{h}_+$ is also not empty and $\mathcal{E} = 1$ on $V \cap \mathfrak{h}_+$. Therefore $\partial(\pi)\mathcal{E}_r = \partial(\pi^{2r+1})\pi^{2r+1} = \langle \pi^{2r+1}, \pi^{2r+1} \rangle$ on $V \cap \mathfrak{h}_+$. But we know from the Corollary to Lemma 18 of [4(d)] that $\langle \pi^{2r+1}, \pi^{2r+1} \rangle$ is a positive constant. This contradiction proves the lemma.

Now in order to prove Lemma 9, we select (see Lemma 9 of [4(d)]) a homogeneous element $\xi \in I(\mathfrak{g})$ of positive degree such that its restriction $\bar{\xi}$

on $\mathfrak{h}$ fulfills the condition of Lemma 10. It is obvious that $\partial(H)\mathcal{E}=0$ for $H\in\sigma$. Moreover,

$$\mathcal{E}(\partial(\alpha_0)(\alpha_0 g))=\int_{\mathfrak{h}_+}\partial(\alpha_0)(\alpha_0 g)\,d\mu=0 \qquad (g\in C_c^\infty(\mathfrak{h}_0)),$$

and therefore $\alpha_0\partial(\alpha_0)\mathcal{E}=0$. We claim that

$$\partial(\alpha_0^k)(\alpha_0^m\mathcal{E})=(\partial(\alpha_0^k)\alpha_0^m)\mathcal{E} \qquad (m\geqq k\geqq 0).$$

This is obviously true for $k=0$. So we assume $k\geqq 1$ and use induction on k. Then $\partial(\alpha_0^{k-1})(\alpha_0^m\mathcal{E})=(\partial(\alpha_0^{k-1})\alpha_0^m)\mathcal{E}$, and therefore

$$\partial(\alpha_0^k)(\alpha_0^m\mathcal{E})=(\partial(\alpha_0^k)\alpha_0^m)\mathcal{E}+(\partial(\alpha_0^{k-1})\alpha_0^m)\partial(\alpha_0)\mathcal{E}=(\partial(\alpha_0^k)\alpha_0^m)\mathcal{E}$$

since $m>k-1$ and $\alpha_0\partial(\alpha_0)\mathcal{E}=0$. Hence if $k>m$,

$$\partial(\alpha_0^k)(\alpha_0^m\mathcal{E})=\partial(\alpha_0^{k-m})\{(\partial(\alpha_0^m)\alpha_0^m)\mathcal{E}\}=\langle\alpha_0^m,\alpha_0^m\rangle\partial(\alpha_0^{k-m})\mathcal{E}.$$

Now consider $\partial(\bar{\xi})\mathcal{E}_r$. Then if

$$\bar{\xi}\pi^{2r}=\sum_{k\geqq 0}\alpha_0^{2r+2k}q_k, \qquad \pi^{2r+1}=\sum_{m\geqq 0}\alpha_0^{2r+1+2m}q_m'$$

$(q_k, q_m'\in S(\sigma))$ as before, it is clear that

$$\begin{aligned}\partial(\bar{\xi})\mathcal{E}_r=\partial(\bar{\xi}\pi^{2r})(\pi^{2r+1}\mathcal{E})&=\sum_{k,m\geqq 0}\partial(\alpha_0^{2r+2k}q_k)(\alpha_0^{2r+1+2m}q_m'\mathcal{E})\\&=\sum_{k,m\geqq 0}(\partial(q_k)q_m')\partial(\alpha_0^{2r+2k})(\alpha_0^{2r+1+2m}\mathcal{E})\\&=\sum_{m\geqq k\geqq 0}(\partial(q_k)q_m')(\partial(\alpha_0^{2r+2k})\alpha_0^{2r+1+2m})\mathcal{E}\\&\quad+\sum_{k>m\geqq 0}(\partial(q_k)q_m')\langle\alpha_0^{2r+1+2m},\alpha_0^{2r+1+2m}\rangle\partial(\alpha_0^{2k-2m-1})\mathcal{E}\end{aligned}$$

since σ and H_{α_0} are orthogonal. Now the first sum is obviously equal to $(\partial(\bar{\xi}\pi^{2r})\pi^{2r+1})\mathcal{E}$. But $\partial(\bar{\xi}\pi^{2r})\pi^{2r+1}$ is a homogeneous polynomial in $S(\mathfrak{h})$ of degree $d^0(\pi)-d^0(\xi)$ which is skew-invariant under W. Therefore it follows from Lemma 10 of [4(d)] that it is zero. Put $\delta^{(k)}=\partial(\alpha_0^{k+1})\mathcal{E}$ $(k\geqq 0)$. Then

$$\partial(\bar{\xi})\mathcal{E}_r=\sum_{k\geqq 0}p_k\delta^{(2k)},$$

where the polynomials $p_k\in S(\sigma)$ are defined as before by

$$p_k=\sum_{m\geqq 0}(\partial(q_{m+1+k})q_m')\langle\alpha_0^{2r+1+2m},\alpha_0^{2r+1+2m}\rangle.$$

On the other hand, since $\partial(\bar{\xi})\mathcal{E}_r\neq 0$, not every p_k can be zero. This completes the proof of Lemma 9.

Now fix r and ξ once for all as in Lemma 9 and let k_0 be an integer such that $p_{k_0}\neq 0$. As before, let $d\mu_\sigma$ denote the Euclidean measure on σ_0.

LEMMA 11. *If U_σ is any open neighborhood of H_0 in σ_0, we can select a function $f \in C_c^\infty(U_\sigma)$ such that*

$$\int_{U_\sigma} f p_k \, d\mu_\sigma = \begin{cases} 0 \text{ if } k \neq k_0, \\ 1 \text{ if } k = k_0 \end{cases} \qquad (k \geqq 0).$$

Let $k_1 < k_2 < \cdots < k_m$ be all the values of k for which $p_k \neq 0$. Then as we have seen p_{k_i} is a homogeneous polynomial in $S(\sigma)$ of degree $d^0(\pi) - d^0(\xi) + 2k_i + 1$ $(1 \leqq i \leqq m)$. Therefore, regarded as functions on $U_\sigma, p_{k_1}, \cdots, p_{k_m}$ are linearly independent over C, and our assertion follows from Lemma 20 of the Appendix (Section 6).

Now let $\mathfrak{a}_1 = \sigma_0 + R^+H'$ and $\mathfrak{b}_0' = \sigma + R'(X' - Y')$ as before. We define the $\mathscr{B}$-distributions (see [4(d), § 2]) $\mathcal{E}_\mathfrak{a}$ and $\mathcal{E}_\mathfrak{b}^\pm$ on $\mathfrak{a}_1$ and $\mathfrak{b}_0'$, respectively, as follows:

$$\mathcal{E}_\mathfrak{a}(g_1) = \int_{\mathfrak{a}_1} g_1 \, d\mu_\mathfrak{a} \qquad (g_1 \in \mathscr{B}(\mathfrak{a}_1)),$$

$$\mathcal{E}_\mathfrak{b}^+(g_2) = \int_{\mathfrak{b}_2} g_2 \, d\mu_\mathfrak{b}, \quad \mathcal{E}_\mathfrak{b}^-(g_2) = \int_{\mathfrak{b}_3} g_2 \, d\mu_\mathfrak{b} \qquad (g_2 \in \mathscr{B}(\mathfrak{b}_0')).$$

Let $\delta_\mathfrak{a}^{(k)} = \partial(\tau^{k+1})\mathcal{E}_\mathfrak{a}$ and ${}^\pm\delta_\mathfrak{b}^{(k)} = \partial(\lambda^{k+1})\mathcal{E}_\mathfrak{b}^\pm$ $(k \geqq 0)$. For any automorphism y of $\mathfrak{g}$ and $p \in S(\mathfrak{g})$, let p^y denote the polynomial function $X \to p(y^{-1}X)$ $(X \in \mathfrak{g})$. Then it is clear that $\pi_\mathfrak{a} = \pi^{\nu_\mathfrak{a}}$, $\pi_\mathfrak{b} = \pi^{\nu_\mathfrak{b}}$ and $p^{\nu_\mathfrak{a}} = p^{\nu_\mathfrak{b}} = p$ for $p \in S(\sigma)$. Moreover, $(\alpha_0)^{\nu_\mathfrak{a}} = \tau$, $(\alpha_0)^{\nu_\mathfrak{b}} = \lambda$ and $(\bar{\xi})^{\nu_\mathfrak{a}} = \xi_\mathfrak{a}$, $(\bar{\xi})^{\nu_\mathfrak{b}} = \xi_\mathfrak{b}$ in the notation of Lemma 8. Therefore

$$\xi_\mathfrak{a}\pi_\mathfrak{a}^{2r} = \sum_{k \geqq 0} \tau^{2r+2k} q_k, \qquad \pi_\mathfrak{a}^{2r+1} = \sum_{m \geqq 0} \tau^{2r+1+2m} q_m'$$

$$\xi_\mathfrak{b}\pi_\mathfrak{b}^{2r} = \sum_{k \geqq 0} \lambda^{2r+2k} q_k, \qquad \pi_\mathfrak{b}^{2r+1} = \sum_{m \geqq 0} \lambda^{2r+1+2m} q_m'.$$

Moreover, it again follows without difficulty that $\partial(H)\mathcal{E}_\mathfrak{a} = 0$, $\partial(H)\mathcal{E}_\mathfrak{b}^\pm = 0$ for $H \in \sigma$ and $\tau\partial(\tau)\mathcal{E}_\mathfrak{a} = 0$, $\lambda\partial(\lambda)\mathcal{E}_\mathfrak{b}^\pm = 0$. Therefore we conclude in the same way as before, that

$$\partial(\xi_\mathfrak{a}\pi_\mathfrak{a}^{2r})(\pi_\mathfrak{a}^{2r+1}\mathcal{E}_\mathfrak{a}) = \sum_{k \geqq 0} p_k \delta_\mathfrak{a}^{(2k)}$$

$$\partial(\xi_\mathfrak{b}\pi_\mathfrak{b}^{2r})(\pi_\mathfrak{b}^{2r+1}\mathcal{E}_\mathfrak{b}) = \sum_{k \geqq 0} p_k {}^\pm\delta_\mathfrak{b}^{(2k)}.$$

Now U being defined as in Lemma 8, let U_σ and $U_\mathfrak{l}$ denote the orthogonal projections of U in σ_0 and $\mathfrak{l}_0$, respectively. Select $g_0 \in C_c^\infty(U_\sigma)$ according to Lemma 11, and for any $\beta \in C_c^\infty(U_\mathfrak{l})$, define $\gamma_\beta \in C_c^\infty(U)$ by

$$\gamma_\beta(H_\sigma + Z) = g_0(H_\sigma)\beta(Z)\,|\,\zeta(H_\sigma + Z)\,|^{-\frac{1}{2}} \qquad (H_\sigma \in U_\sigma, Z \in U_\mathfrak{l}).$$

Moreover, let $F_\beta = f_{\gamma_\beta}$ (in the notation of Lemmas 1 and 8) and

$$\phi_\beta(t) = \int_{-\infty}^{\infty} \bar{\beta}(tH' + xX')\,dx \qquad (t \in R^+)$$

$$\psi_\beta(s) = |s| \int_0^{\infty} \bar{\beta}(s(e^tX' - e^{-t}Y'))\,(e^t - e^{-t})\,dt \qquad (s \in R');$$

where[2] $\bar{\beta}(Z) = \pi^{-1}\int_0^{\pi} \beta(u_tZ)\,dt$ and $u_t = \exp(t\,\mathrm{ad}(X' - Y'))$. Put $\phi_\beta(0) = \operatorname*{Lim}_{t\to 0} \phi_\beta(t)$ $(t \in R^+)$, $\psi_\beta^+(0) = \operatorname*{Lim}_{s\to 0} \psi_\beta(s)$ $(s \in R^+)$ and $\psi_\beta^-(0) = \operatorname*{Lim}_{s\to 0} \psi_\beta(s)$ $(s \in R^-)$. All these limits exist (see Section 6). Also let π' denote the product of all roots $\alpha \neq \alpha_0$ in P. Then $\pi'(H_0) \neq 0$. We set $\epsilon = |\pi'(H_0)|/\pi'(H_0)$.

LEMMA 12. *Let* $q = d^0(\xi)$ *and* $a = \epsilon(-1)^q\{\alpha_0(H_{\alpha_0})\}^{2k_0+1}2^{k_0-2}$, *where* k_0 *has the same meaning as in Lemma* 11. *Then for any* $\beta \in C_c^\infty(U_{\mathrm{I}})$,

$$\int_{N_1} \eta^r \partial(\eta^r\xi) F_\beta dX = a\phi_{\beta_0}(0),$$

where $\beta_0 = \partial(\Omega^{k_0})\beta$. *Similarly,*

$$\int_{N^\pm} \eta^r \partial(\eta^r\xi) F_\beta dX = -a\psi_{\beta_0}^{\pm}(0)$$

if $[\Xi : LB] = 1$, *and, if* $[\Xi : LB] = 2$,

$$\int_{N_2 \cup N_3} \eta^r \partial(\eta^r\xi) F_\beta dX = -a\{\psi_{\beta_0}^+(0) + \psi_{\beta_0}^-(0)\}.$$

Define $\epsilon_{\mathfrak{a}}$ and $\epsilon_{\mathfrak{b}}$ on $\mathfrak{a}_1 \cap U$ and $\mathfrak{b}_0' \cap U$ as in the Corollary to Lemma 8. Then $\epsilon_{\mathfrak{a}}$ is constant on $\mathfrak{a}_1 \cap U$ and $\epsilon_{\mathfrak{b}}$ on $\mathfrak{b}_i \cap U$ $(i = 2, 3)$, and it is obvious that $\pi_{\mathfrak{a}}'(H_0) = \pi_{\mathfrak{b}}'(H_0) = \pi'(H_0) \neq 0$, where $\pi_{\mathfrak{a}}' = (\pi')^{\nu_{\mathfrak{a}}}$, $\pi_{\mathfrak{b}}' = (\pi')^{\nu_{\mathfrak{b}}}$. Therefore since $\pi_{\mathfrak{a}} = \tau\pi_{\mathfrak{a}}'$, by making H tend to H_0 $(H \in \mathfrak{a}_1 \cap U)$, we conclude immediately that $\epsilon_{\mathfrak{a}} = \epsilon$. Similarly, $\epsilon_{\mathfrak{b}} = -(-1)^{\frac{1}{2}}\epsilon$ and $(-1)^{\frac{1}{2}}\epsilon$ on $\mathfrak{b}_2$ and $\mathfrak{b}_3$, respectively. Hence it follows from the Corollary to Lemma 8 that

$$\int_{N_1} \eta^r \partial(\eta^r\xi) F_\beta dX = \tfrac{1}{2}\epsilon\mathcal{E}_{\mathfrak{a}}(\pi_{\mathfrak{a}}^{2r+1}\partial(\pi_{\mathfrak{a}}^{2r}\xi_{\mathfrak{a}})\Phi_{|\zeta|^{\frac{1}{2}}\gamma_\beta})$$
$$= \tfrac{1}{2}\epsilon(-1)^q \sum_{k\geqq 0} \delta_{\mathfrak{a}}^{(2k)}(p_k\Phi_{|\zeta|^{\frac{1}{2}}\gamma_\beta}) = -\tfrac{1}{2}\epsilon(-1)^q \sum_{k\geqq 0} \mathcal{E}_{\mathfrak{a}}(p_k\partial(\tau^{2k+1})\Phi_{|\zeta|^{\frac{1}{2}}\gamma_\beta})$$

in view of our result above. But it is clear that

$$\Phi_{|\zeta|^{\frac{1}{2}}\gamma_\beta}(H_\sigma + tH') = g_0(H_\sigma)\psi_\beta(t) \qquad (H_\sigma \in U_\sigma, t \in R^+).$$

Let H_τ denote the element in $\mathfrak{a}$ such that $B(H, H_\tau) = \tau(H)$ for all $H \in \mathfrak{a}$. Then it is clear that $\tau(H_\tau) = \alpha_0(H_{\alpha_0}) = \langle\alpha_0, \alpha_0\rangle$, and hence $H_\tau = \frac{1}{2}\langle\alpha_0, \alpha_0\rangle H'$. Therefore

$$\mathcal{E}_{\mathfrak{a}}(p_k\partial(\tau^{2k+1})\Phi_{|\zeta|^{\frac{1}{2}}\gamma_\beta})$$
$$=\langle\alpha_0,\alpha_0\rangle^{2k+1}2^{-(2k+1)}\int_{U\sigma}p_kg_0d\mu_\sigma\int_0^\infty(d^{2k+1}\phi_\beta/dt^{2k+1})\,dt.$$

On the other hand, we know from Lemma 17 (Appendix, Section 6) that

$$\phi_{\partial(\Omega^k)\beta}=2^{-3k}d^{2k}\phi_\beta/dt^{2k}.$$

So it follows from the definition of g_0 that

$$\int_{N_1}\eta^r\partial(\eta^r\xi)F_\beta\,dX=\epsilon\langle\alpha_0,\alpha_0\rangle^{2k_0+1}2^{k_0-2}(-1)^q\phi_{\beta_0}(0),$$

and this proves the first formula.

Now suppose $[\Xi\colon LB]=1$. Then it follows again from the Corollary to Lemma 8 that

$$\int_{N^\pm}\eta^r\partial(\eta^r\xi)F_\beta dX=\mp\tfrac{1}{2}\epsilon(-1)^{\frac{1}{2}}\mathcal{E}_{\mathfrak{b}}^\pm(\pi_{\mathfrak{b}}^{2r+1}\partial(\pi_{\mathfrak{b}}^{2r}\xi_{\mathfrak{b}})\Psi_{|\zeta|^{\frac{1}{2}}\gamma_\beta})$$
$$=\mp\tfrac{1}{2}\epsilon(-1)^{q+\frac{1}{2}}\sum_{k\geqq 0}{}^{\pm}\delta_{\mathfrak{b}}^{(2k)}(p_k\Psi_{|\zeta|^{\frac{1}{2}}\gamma_\beta})=\pm\tfrac{1}{2}\epsilon(-1)^{q+\frac{1}{2}}\sum_{k\geqq 0}\mathcal{E}_{\mathfrak{b}}^\pm(p_k\partial(\lambda^{2k+1})\Psi_{|\zeta|^{\frac{1}{2}}\gamma_\beta}).$$

Let H_λ denote the element in $\mathfrak{b}$ such that $B(H,H_\lambda)=\lambda(H)$ $(H\in\mathfrak{b})$. Then $\lambda(H_\lambda)=\alpha_0(H_{\alpha_0})=\langle\alpha_0,\alpha_0\rangle$ and $H_\lambda=\nu_{\mathfrak{b}}H_{\alpha_0}=-\frac{1}{2}(-1)^{\frac{1}{2}}\langle\alpha_0,\alpha_0\rangle(X'-Y')$. Therefore

$$\mathcal{E}_{\mathfrak{b}}^+(p_k\partial(\lambda^{2k+1})\Psi_{|\zeta|^{\frac{1}{2}}\gamma_\beta})$$
$$=\langle\alpha_0,\alpha_0\rangle^{2k+1}(-1)^{k-\frac{1}{2}}2^{-(2k+1)}\int_{U\sigma}p_kg_0d\mu_\sigma\int_0^\infty(d^{2k+1}\psi_\beta/dt^{2k+1})\,dt$$

and

$$\mathcal{E}_{\mathfrak{b}}^-(p_k\partial(\lambda^{2k+1})\Psi_{|\zeta|^{\frac{1}{2}}\gamma_\beta})$$
$$=\langle\alpha_0,\alpha_0\rangle^{2k+1}(-1)^{k-\frac{1}{2}}2^{-(2k+1)}\int_{U\sigma}p_kg_0d\mu_\sigma\int_{-\infty}^0(d^{2k+1}\psi_\beta/dt^{2k+1})\,dt.$$

On the other hand,

$$\psi_{\partial(\Omega^k)\beta}=(-1)^k2^{-3k}d^{2k}\psi_\beta/dt^{2k}$$

from Lemma 17 (Section 6). Therefore

$$\mathcal{E}_{\mathfrak{b}}^\pm(p_k\partial(\lambda^{2k+1})\Psi_{|\zeta|^{\frac{1}{2}}\gamma_\beta})$$
$$=\pm\langle\alpha_0,\alpha_0\rangle^{2k+1}(-1)^{\frac{1}{2}}2^{k-1}\psi_{\partial(\Omega^k)\beta}^{\pm}(0)\int_{U\sigma}p_kg_0d\mu_\sigma,$$

and by taking into account the definition of g_0 we get,

$$\int_{N^\pm}\eta^r\partial(\eta^r\xi)F_\beta\,dX=-\epsilon\langle\alpha_0,\alpha_0\rangle^{2k_0+1}(-1)^q2^{k_0-2}\psi_{\beta_0}^{\pm}(0).$$

Finally, suppose $[\Xi : LB] = 2$. Then again from the Corollary to Lemma 8,

$$\int_{N_2 \cup N_3} \eta^r \partial(\eta^r \xi) F_\beta \, dX = -\tfrac{1}{2}\epsilon(-1)^{\frac{1}{2}} \mathcal{E}_{\mathfrak{b}} (\pi_{\mathfrak{b}}{}^{2r+1} \partial(\pi_{\mathfrak{b}}{}^{2r} \xi_{\mathfrak{b}}) \Psi_{|\zeta|^{\frac{1}{2}}\gamma_\beta}),$$

where $\mathcal{E}_{\mathfrak{b}} = \mathcal{E}_{\mathfrak{b}}{}^+ - \mathcal{E}_{\mathfrak{b}}{}^-$, and we conclude from the above caluculation that

$$\int_{N_2 \cup N_3} \eta^r \partial(\eta^r \xi) F_\beta \, dX = -\epsilon \langle \alpha_0, \alpha_0 \rangle^{2k_0+1} (-1)^q 2^{k_0-2} [\psi_{\beta_0}{}^+(0) + \psi_{\beta_0}{}^-(0)].$$

This completes the proof of Lemma 12.

We are now in a position to prove the main result of this section.

THEOREM 1. *Let r and ξ be defined as in Lemma 9 and let c_1, c_2, c_3 be three complex numbers. We assume that $c_2 = c_3$ in case $[\Xi : LB] = 2$. Let N_0 be an open neighborhood of H_0 in N and let T be the distribution on N_0 defined as follows:*

$$T(f) = \sum_{1 \leqq i \leqq 3} c_i \int_{N_i} \eta^r \partial(\eta^r) f dX \qquad (f \in C_c{}^\infty(N_0)).$$

Then $\partial(\xi) T = 0$ implies that $c_1 = c_2 = c_3$.

Let ${}_0U$ be an open neighborhood of H_0 in U and ${}_0V^*$ an open neighborhood of 1^* in V^* (see Lemma 1 for the definition of V^*). We can choose ${}_0V^*$ and ${}_0U$ so small that $\phi(x^*)Z \in N_0$ for $x^* \in {}_0V^*$, $Z \in {}_0U$. Let ${}_0U_\sigma$ and ${}_0U_{\mathfrak{l}}$ be the orthogonal projections of ${}_0U$ in σ_0 and $\mathfrak{l}_0$, respectively. We may further assume that ${}_0U = {}_0U_\sigma + {}_0U_{\mathfrak{l}}$. Moreover, we can suppose that the carriers of the functions a_0 and g_0 (used in the definitions of f_γ and F_β in Lemmas 1 and 12, respectively) are contained in ${}_0V^*$ and ${}_0U_\sigma$, respectively. Then it is clear that $F_\beta \in C_c{}^\infty(N_0)$ for any $\beta \in C_c{}^\infty({}_0U_{\mathfrak{l}})$, and therefore $T(\partial(\xi)F_\beta) = 0$ by our hypothesis. On the other hand, it follows from Lemma 12 that

$$T(\partial(\xi)F_\beta) = a\{c_1 \phi_{\partial(\Omega^{k_0})\beta}(0) - c_2 \psi^+{}_{\partial(\Omega^{k_0})\beta}(0) - c_3 \psi^-{}_{\partial(\Omega^{k_0})\beta}(0)\}$$

since $c_2 = c_3$ when $[\Xi : LB] = 2$. Now put $\beta = \Omega^{k_0}\gamma$ $(\gamma \in C_c{}^\infty({}_0U_{\mathfrak{l}}))$ and $\gamma_0 = \partial(\Omega^{k_0})(\Omega^{k_0}\gamma)$. Then it is clear that

$$c_1 \phi_{\gamma_0}(0) - c_2 \psi_{\gamma_0}{}^+(0) - c_3 \psi_{\gamma_0}{}^-(0) = 0$$

for all $\gamma \in C_c{}^\infty({}_0U_{\mathfrak{l}})$. On the other hand if $c = 2^{2k_0} k_0! \Gamma(k_0 + \frac{1}{2}) / \Gamma(\frac{1}{2})$, it follows from the Corollary of Lemma 18 (Section 6) that $\phi_{\gamma_0}(0) = c\phi_\gamma(0)$, $\psi_{\gamma_0}{}^\pm(0) = c\psi_\gamma{}^\pm(0)$. Therefore, since c is positive, we conclude that

$$c_1 \phi_\gamma(0) - c_2 \psi_\gamma{}^+(0) - c_3 \psi_\gamma{}^-(0) = 0$$

for all $\gamma \in C_c^\infty({}_0U_\mathrm{I})$, and now it follows from Lemma 19 (Section 6) that $c_1 = c_2 = c_3$.

4. Proof of Theorem 2. We shall now apply Theorem 1 to prove that the constants $c_1, \cdots, c_N$ of Lemma 29 of [4(e)] are all equal. But first we need one additional fact.

LEMMA 13. *Let S denote the set of those elements in $\mathfrak{g}_0$ which are either regular or semiregular. Then S is connected.*

Suppose V_1, V_2 are two closed subsets of $\mathfrak{g}_0$ such that $V_1 \cup V_2 = \mathfrak{g}_0$ and $V_1 \cap V_2 \cap S = \emptyset$. Then we have to show that S is contained in one of the two sets V_1, V_2. Let $\mathfrak{h}_0$ be a Cartan subalgebra of $\mathfrak{g}_0$ such that $\theta(\mathfrak{h}_0) = \mathfrak{h}_0$. We use the notation of Section 2. For any root $\alpha \in P$, let σ_α denote the set of those $H \in \mathfrak{h}_0$ where $\alpha(H) = 0$. Moreover, let U be the complement in $\mathfrak{h}_0$ of the union of the sets $\sigma_\alpha \cap \sigma_\beta$ $(\alpha, \beta \in P;\ \alpha \neq \beta)$. Then U is connected (see the Corollary to Lemma 42 of [4(e)]), and it is obvious that $U \subset S$. Therefore U is contained in one of the two sets V_1, V_2. But since U is dense in $\mathfrak{h}_0$, we conclude that either V_1 or V_2 contains $\mathfrak{h}_0$.

Let X be an element in S. Then since G is connected, $\bigcup_{x \in G} xX$ is a connected subset of S. Then if $X \in V_i$, it follows that $xX \in V_i$ for every $x \in G$ $(i = 1, 2)$. Now select i such that $\mathfrak{h}_0 \subset V_i$. Then $x(\mathfrak{h}_0 \cap \mathfrak{g}_0') \subset V_i$ $(x \in G)$, and therefore since $\mathfrak{h}_0 \cap \mathfrak{g}_0'$ is dense in $\mathfrak{h}_0$, $x\mathfrak{h}_0 \subset V_i$.

Let $\mathfrak{a}_0$ be a fundamental Cartan subalgebra (see [4(e), § 8]) of $\mathfrak{g}_0$ such that $\mathfrak{a}_0 = \theta(\mathfrak{a}_0)$. We may assume that $\mathfrak{a}_0 \subset V_1$. For any Cartan subalgebra $\mathfrak{r}_0$ of $\mathfrak{g}_0$, define $l_-(\mathfrak{r}_0)$ as in [4(e), § 8]. We shall prove by induction on $l_-(\mathfrak{a}_0) - l_-(\mathfrak{h}_0)$ that $\mathfrak{h}_0 \subset V_1$. If $l_-(\mathfrak{a}_0) = l_-(\mathfrak{h}_0)$, $\mathfrak{h}_0$ is also fundamental and therefore conjugate to $\mathfrak{a}_0$ under G (see the Corollary to Lemma 32 of [4(e)]). Hence it follows from what has been said above that $\mathfrak{h}_0 \subset V_1$. So let us now suppose that $l_-(\mathfrak{h}_0) < l_-(\mathfrak{a}_0)$. Since K is compact and $\mathfrak{a}_0 \cap \mathfrak{k}_0$ is a maximal abelian subalgebra of $\mathfrak{k}_0$ (Corollary to Lemma 31 of [4(e)]), we may assume (by replacing $\mathfrak{h}_0$ by a conjugate Cartan subalgebra) that $\mathfrak{h}_0 \cap \mathfrak{k}_0 \subset \mathfrak{a}_0 \cap \mathfrak{k}_0$. Let $\mathfrak{q}_0$ be the centralizer of $\mathfrak{h}_0 \cap \mathfrak{k}_0$ in $\mathfrak{g}_0$. Then obviously $\theta(\mathfrak{q}_0) = \mathfrak{q}_0$ and therefore $\mathfrak{q}_0$ is reductive in $\mathfrak{g}_0$ (Lemma 10 of [4(e)]). Moreover, since $\mathfrak{h}_0$ is maximal abelian in $\mathfrak{g}_0$, it is clear that $\mathfrak{h}_0 \cap \mathfrak{p}_0$ is a maximal abelian subspace of $\mathfrak{q}_0 \cap \mathfrak{p}_0$. Let L be the connected component of 1 in the centralizer of $\mathfrak{h}_0 \cap \mathfrak{k}_0$ in K. Then L is compact and its Lie algebra is $\mathfrak{q}_0 \cap \mathfrak{k}_0$. Moreover, since $\mathfrak{q}_0$ is reductive and $\theta(\mathfrak{q}_0) = \mathfrak{q}_0$, any two maximal abelian subspaces of $\mathfrak{q}_0 \cap \mathfrak{p}_0$ are conjugate under L (see Cartan [1] or Lemma 39 of

[4(b)]). Therefore since $\mathfrak{a}_0 \cap \mathfrak{p}_0 \subset \mathfrak{q}_0' \cap \mathfrak{p}_0$, we can select $k \in L$ such that $\mathfrak{a}_0 \cap \mathfrak{p}_0 \subset k(\mathfrak{h}_0 \cap \mathfrak{p}_0)$. Then by replacing $\mathfrak{h}_0$ by $k\mathfrak{h}_0$ we can assume that $\mathfrak{h}_0 \cap \mathfrak{p}_0 \supset \mathfrak{a}_0 \cap \mathfrak{p}_0$ and $\mathfrak{h}_0 \cap \mathfrak{k}_0 \subset \mathfrak{a}_0 \cap \mathfrak{k}_0$. Now since $\mathfrak{h}_0$ is not fundamental, there exists a root $\alpha_0 \in P$ which takes only real values on $\mathfrak{h}_0$ (see Lemma 33 of [4(e)]), and we can assume that $X_{\alpha_0}, X_{-\alpha_0} \in \mathfrak{g}_0$ and $X_{\alpha_0} - X_{-\alpha_0} \in \mathfrak{k}_0$ (Lemma 46 of [4(e)]). Then $\mathfrak{h}_1 = \sigma_{\alpha_0} + R(X_{\alpha_0} - X_{-\alpha_0})$ is a Cartan subalgebra of $\mathfrak{g}_0$ and $\theta(\mathfrak{h}_1) = \mathfrak{h}_1$. Since α_0 is identically zero on $\mathfrak{h}_0 \cap \mathfrak{k}_0$, it follows that $\sigma_{\alpha_0} \supset \mathfrak{h}_0 \cap \mathfrak{k}_0$, and therefore $l_{-}(\mathfrak{h}_1) \geqq l_{-}(\mathfrak{h}_0) + 1$. Hence $\mathfrak{h}_1 \subset V_1$ by our induction hypothesis. On the other hand, we can obviously choose a point $H \in \sigma_{\alpha_0}$ such that $\alpha(H) \neq 0$ for any root $\alpha \neq \alpha_0$ in P. Then H is semiregular and therefore $\mathfrak{h}_0 \cap \mathfrak{h}_1 \cap S \neq \emptyset$. But since $V_1 \cap V_2 \cap S = \emptyset$, we conclude that $\mathfrak{h}_0$ must also be contained in V_1.

Now let X be any element in $\mathfrak{g}_0'$ and let $\mathfrak{h}_X$ denote its centralizer in $\mathfrak{g}_0$. Then $\mathfrak{h}_X$ is a Cartan subalgebra of $\mathfrak{g}_0$ and some conjugate of $\mathfrak{h}_X$ (under G) is invariant under θ (see [4(c), Corollary to Lemma 1]). Hence it follows from our result that $\mathfrak{h}_X \subset V_1$. Therefore, since $X \in \mathfrak{h}_X$ and $\mathfrak{g}_0'$ is dense in $\mathfrak{g}_0$, we conclude that $V_1 = \mathfrak{g}_0$. This proves that $S \subset V_1$.

Define $\mathfrak{h}_0$ and T' as in Lemma 27 of [4(e)]. Then T' is a distribution on $\mathfrak{g}_0$.

LEMMA 14. *There exists an open neighborhood V of S in $\mathfrak{g}_0$ and a constant c' such that $T' = c'$ on V.*

Since S is connected, it would be sufficient to prove that T' coincides with a constant on some open neighborhood (in $\mathfrak{g}_0$) of any point $X_0 \in S$. If X_0 is regular, this follows from Lemma 27 of [4(e)]. So now suppose that X_0 is semiregular. Then since $\operatorname{ad} X_0$ is semisimple, X_0 is contained in some Cartan subalgebra $\mathfrak{a}_0$ of $\mathfrak{g}_0$. Select $x \in G$ such that $\theta(x\mathfrak{a}_0) = x\mathfrak{a}_0$ (see the Corollary to Lemma 1 of [4(c)]), and put $H_0 = xX_0$, $x\mathfrak{a}_0 = \mathfrak{b}_0$. Then since T' is invariant under G, it would be sufficient to prove that T' coincides with a constant on some neighborhood of H_0. On the other hand, we know from Lemma 30 of [4(e)] that $\partial(\xi)T' = 0$ for any homogeneous element $\xi \in I(\mathfrak{g})$ of positive degree. Now select a neighborhood N of H_0 corresponding to Lemmas 1 and 2, and let $\mathfrak{g}_i$ $(1 \leqq i \leqq k)$ be all the distinct connected components of $\mathfrak{g}_0'$ which meet N. Then $k \leqq 3$ from Lemma 2. Moreover, it follows from Lemma 29 of [4(e)] that there exists an open neighborhood N_0 of H_0 in N, an integer $r \geqq 0$ and complex numbers c_i $(1 \leqq i \leqq k)$ such that

$$\langle \eta^r, \eta^r \rangle T'(f) = \sum_{1 \leqq i \leqq k} c_i \int_{N \cap \mathfrak{g}_i} \eta^r \partial(\eta^r) f \, dX$$

for all $f \in C_c^\infty(N_0)$. Now the set of singular elements of $\mathfrak{g}_0$ obviously has Euclidean measure zero. Therefore if $k=1$, it is obvious that

$$\langle \eta^r, \eta^r \rangle T'(f) = c_1 \int_{\mathfrak{g}_0} \eta^r \partial(\eta^r) f \, dX = c_1 \langle \eta^r, \eta^r \rangle \int_{\mathfrak{g}_0} f \, dX,$$

since η is a homogeneous polynomial of even degree. Moreover, $\langle \eta^r, \eta^r \rangle \neq 0$ (Corollary to Lemma 18 of [4(d)]). Therefore $T' = c_1$ on N_0 in this case. So let us now assume that $k \geqq 2$. Then we may obviously suppose that N is chosen in accordance with Lemma 8. Select ξ corresponding to Lemma 9 and let us use the notation of Theorem 1. If $[\Xi : LB] = 2$, we know from Lemma 7 that there exists an element $x \in \Xi$ such that $x(X' - Y') = -(X' - Y')$. On the other hand, if t is positive and sufficiently small, $H_0 + t(X' - Y') \in N_2$ while $x(H_0 + t(X' - Y')) = H_0 - t(X' - Y') \in N_3$. Moreover, since G is connected, the points $y(H_0 + t(X' - Y'))$ $(y \in G)$ are all contained in the same connected component of $\mathfrak{g}_0'$. Therefore it is clear that both N_2 and N_3 lie in the same connected component of $\mathfrak{g}_0'$. Hence $k = 2$ in this case. This shows that

$$\langle \eta^r, \eta^r \rangle T'(f) = \sum_{1 \leqq i \leqq 3} c_i' \int_{N_i} \eta^r \partial(\eta^r) f \, dX \qquad (f \in C_c^\infty(N_0))$$

(in the notation of Theorem 1) where c_1', c_2', c_3' are certain constants and $c_2' = c_3'$ in case $[\Xi : LB] = 2$. Furthermore, $\partial(\xi) T' = 0$ as we have already observed above. Hence it follows from Theorem 1 that $c_1' = c_2' = c_3'$, and therefore

$$\langle \eta^r, \eta^r \rangle T'(f) = c_1' \int_N \eta^r \partial(\eta^r) f \, dX = c_1' \langle \eta^r, \eta^r \rangle \int_{\mathfrak{g}_0} f \, dX$$

for all $f \in C_c^\infty(N_0)$. This proves that T' coincides with c_1' on N_0.

We can now prove the following theorem.

THEOREM 2. *Let* $\mathfrak{h}_0$ *be a Cartan subalgebra of* $\mathfrak{g}_0$ *such that*[3] $\theta(\mathfrak{h}_0) = \mathfrak{h}_0$ *and* $\mathfrak{h}_1$ *a connected component of* $\mathfrak{h}_0' = \mathfrak{h}_0 \cap \mathfrak{g}_0'$. *For any* $f \in \mathcal{E}(\mathfrak{g}_0)$, *put*

$$\phi_f(H) = \pi(H) \int_{G^*} f(x^* H) \, dx^* \qquad (H \in \mathfrak{h}_0')$$

in the notation of Theorem 3 *of* [4(e)]. *Then there exists a real number* c *such that*

$$\lim_{H \to 0} \phi_f(H ; \partial(\pi)) = c f(0) \qquad (H \in \mathfrak{h}_1)$$

for all $f \in \mathcal{E}(\mathfrak{g}_0)$. *Moreover* $c = 0$ *if* $\mathfrak{h}_0$ *is not fundamental.*

---

[3] In view of the Corollary to Lemma 1 of [4(c)], the assumption $\theta(\mathfrak{h}_0) = \mathfrak{h}_0$ is obviously unnecessary. However, we make it here for convenience.

Since $\mathfrak{g}_0' \subset S$, it follows from Lemma 14 that $T' = c'$ on $\mathfrak{g}_0'$. Hence we conclude from the Corollary to Lemma 29 of [4(e)] that $T' = c'$ on $\mathfrak{g}_0$. In view of the definition of T', this implies that

$$\operatorname*{Lim}_{\mathfrak{h}_1} \phi_f(0;\partial(\pi)) = cf(0) \qquad (f \in \mathscr{C}(\mathfrak{g}_0)),$$

where c is a complex number independent of f. We know that η takes only real values on $\mathfrak{g}_0$ (see [4(e), § 6]). Select an element $H_0 \in \mathfrak{h}_0'$ and put $\epsilon = |\pi(H_0)|/\pi(H_0)$. Then it is clear that $\epsilon\pi$ takes only real values on $\mathfrak{h}_0'$. Let us choose a real-valued function $f \in \mathscr{C}(\mathfrak{g}_0)$ such that $f(0) = 1$. Then obviously $\partial(\epsilon\pi)(\epsilon\phi_f) = \epsilon^2\partial(\pi)\phi_f$ takes only real values on $\mathfrak{h}_0'$. Since $\epsilon^2 = \pm 1$, it follows that $c = \operatorname*{Lim}_{\mathfrak{h}_1} \phi_f(0;\partial(\pi))$ is real. Finally we know from the Corollary to Lemma 34 of [4(e)] that $c = 0$ if $\mathfrak{h}_0$ is not fundamental.

5. Proof of Theorem 3. Our next object is to prove the following theorem.

THEOREM 3. *Let* $\mathfrak{h}_0$ *be a fundamental Cartan subalgebra of* $\mathfrak{g}_0$ *such that*[3] $\theta(\mathfrak{h}_0) = \mathfrak{h}_0$. *Let* $\mathfrak{h}_{(1)}, \cdots, \mathfrak{h}_{(q)}$ *be all the distinct connected components of* $\mathfrak{h}_0' = \mathfrak{h}_0 \cap \mathfrak{g}_0'$ *and* $c_1, \cdots, c_q$ *the corresponding real numbers of Theorem 2. Then* $c_1 + c_2 + \cdots + c_q \neq 0$.

If the ranks of $\mathfrak{g}$ and $\mathfrak{k}$ are equal, this follows immediately from Lemma 41 of [4(e)] and Theorem 2. So let us now suppose that $\operatorname{rank} \mathfrak{g} > \operatorname{rank} \mathfrak{k}$. We use the notation of [4(e), § 5] and put $\mathfrak{g}_1 = \bigcup_{x \in G} x\mathfrak{h}_0'$. Then if the invariant measure dx^* on G/A is suitably normalized,

$$\int_{\mathfrak{g}_1} f(X)\,dX = \int_{G^* \times \mathfrak{h}_0'} f(x^*H)\,|\pi(H)|^2\,dx^*dH$$

for $f \in C_c(\mathfrak{g}_1)$. Here dX and dH are the regular Euclidean measures on $\mathfrak{g}_0$ and $\mathfrak{h}_0$, respectively. On the other hand, it follows from the Corollary to Lemma 15 of [4(e)] that

$$\int_{G^*} f(x^*H)\,dx^* = |\pi_+(H)|^{-1} \int f(k(mH + Z))\,dk\,dm\,dZ$$

for $H \in \mathfrak{h}_0'$ and $f \in \mathscr{C}(\mathfrak{g}_0)$. Here $\pi_+ = \prod_{\alpha \in P_+} \alpha$, dk, dm are the Haar measures on K and M, respectively, and dZ is the Euclidean measure on $\mathfrak{n}_0$. Moreover $\int_K dk = 1$. Since $\mathfrak{h}_0$ is fundamental, no root in P can vanish identically on $\mathfrak{h}_0 \cap \mathfrak{k}_0$ (see Lemma 33 of [4(e)]). Therefore $\alpha \neq -\theta\alpha$ for $\alpha \in P_+$. On the other hand, since α and $-\theta\alpha$ coincide on $\mathfrak{h}_{\mathfrak{p}_0}$, it follows from the

Then it follows from Lemma 19 of [4(e)] that $\psi_g \in \mathcal{C}(\mathfrak{h}_0'')$ and $\partial(\pi_+)\psi_g = \psi_{\partial(\zeta)g}$. On the other hand, we know from Theorem 2 (applied to $\mathfrak{l}_0$) that there exist constants c_i' $(1 \leqq i \leqq q)$ such that

$$\operatorname*{Lim}_{H\to 0} \psi_g(H;\partial(\pi')) = c_i' g(0) \qquad (H \in \mathfrak{h}_{(i)}'')$$

for every $g \in \mathcal{C}(\mathfrak{l}_0)$. Moreover, since $\mathfrak{h}_0 \cap \mathfrak{k}_0$ is maximal abelian in $\mathfrak{m}_0$, we conclude from Lemma 41 of [4(e)] (applied to $[\mathfrak{l}_0, \mathfrak{l}_0]$) that $c_1' + \cdots + c_q' \neq 0$. Now put

$$\bar{F}_1(X) = \int_K \bar{F}(kX)\,dk \quad (X \in \mathfrak{g}_0) \quad \text{and} \quad g_1(L) = \int_{\mathfrak{n}_0} \bar{F}_1(L+Z)\,dZ \quad (L \in \mathfrak{l}_0).$$

Then $\phi_{\bar{F}} = \psi_{g_1}$, and therefore $\partial(\pi)\phi_{\bar{F}} = \partial(\pi')\psi_{\partial(\zeta)g_1}$ on $\mathfrak{h}_0'$. Hence

$$\operatorname*{Lim}_{H\to 0} \phi_{\bar{F}}(H;\partial(\pi)) = \operatorname*{Lim}_{H\to 0} \psi_{\partial(\zeta)g_1}(H;\partial(\pi')) = c_i' g_1(0;\partial(\zeta)) \qquad (H \in \mathfrak{h}_{(i)}).$$

Now put $F_1(X) = \int_K F(kX)\,dk$ $(X \in \mathfrak{g}_0)$. Then since $\mathfrak{g}_0$ is the orthogonal sum of $\mathfrak{n}_0$, $\mathfrak{l}_0$ and $\theta(\mathfrak{n}_0)$, we conclude from the theory of Fourier transforms that

$$\begin{aligned} g_1(L') &= \int_{\mathfrak{n}_0} \bar{F}_1(L'+Z)\,dZ \\ &= \int_{\mathfrak{l}_0 \times \mathfrak{n}_0} \exp\{(-1)^{\frac{1}{2}} B(L', L)\} F_1(L+Z)\,dL\,dZ \qquad (L' \in \mathfrak{l}_0). \end{aligned}$$

Here dL is the (suitably normalized) Euclidean measure on $\mathfrak{l}_0$. Hence it follows easily that

$$g_1(0;\partial(\zeta)) = (-1)^{r_+/2} \int_{\mathfrak{l}_0 \times \mathfrak{n}_0} \zeta(L) F_1(L+Z)\,dL\,dZ,$$

where r_+ is the number of roots in P_+. Select $L \in \mathfrak{l}_0$ and $Z \in \mathfrak{n}_0$ such that $\zeta(L)F_1(L+Z) \neq 0$. Then it follows from Lemma 16 of [4(e)] that $nL = L + Z = xH$ for some $n \in N$, $x \in G$ and $H \in \mathfrak{h}_0'$. Hence $L = yH$ if $y = n^{-1}x$. Let $\mathfrak{h}_L$ denote the centralizer of L in $\mathfrak{g}_0$. Then $\mathfrak{h}_L = y\mathfrak{h}_0$, and therefore $\mathfrak{h}_L$ is a fundamental Cartan subalgebra of $\mathfrak{g}_0$. On the other hand, since the ranks of $\mathfrak{l}_0$ and $\mathfrak{g}_0$ are the same, it is evident that $\mathfrak{h}_L \subset \mathfrak{l}_0$, and therefore, obviously, both $\mathfrak{h}_0$ and $\mathfrak{h}_L$ are fundamental Cartan subalgebras[5] of the reductive algebra $\mathfrak{l}_0$. Hence it follows from the Corollary to Lemma 32 of [4(e)] that $\mathfrak{h}_L = m\mathfrak{h}_0$ for some $m \in M$. Since L is a regular element of $\mathfrak{h}_L$, we conclude that $L = mH_1$ for some $H_1 \in \mathfrak{h}_0'$, and therefore $\zeta(L) = \zeta(H_1) = \pi_+(H_1) > 0$. This shows that

---

[5] The notion of a fundamental Cartan subalgebra is extended to reductive Lie algebras over R in the obvious way.

$$g_1(0;\partial(\zeta)) = \epsilon \int |\zeta(L)| F_1(L+Z)\,dLdZ = \epsilon \int_{\mathfrak{l}_0 \times N} |\zeta(L)|^2 F_1(nL)\,dLdn$$

from Lemma 15 of [4(e)]. (Here $\epsilon = (-1)^{r_+/2}$.) Now put $\mathfrak{l}_1 = \bigcup_{m \in M} m(\mathfrak{h}_0')$. Then as we have seen above, $\zeta(L)F_1(nL) = 0$ $(n \in N, L \in \mathfrak{l}_0)$ unless $L \in \mathfrak{l}_1$. Moreover, it is clear that there exists a positive constant a such that

$$\int_{\mathfrak{l}_1} f(L)\,dL = a \int'_{M \times \mathfrak{h}_0'} f(mH)\,|\pi'(H)|^2\,dmdH$$

for all $f \in C_c^\infty(\mathfrak{l}_1)$. Hence

$$\begin{aligned} g_1(0;\partial(\zeta)) &= a\epsilon \int |\zeta(H)|^2 F_1(nmH)\,|\pi'(H)|^2\,dmdHdn \\ &= a\epsilon \int |\pi(H)|^2 F(knmH)\,dkdmdHdn \\ &= a\epsilon \int |\pi(H)|^2 F(x^*H)\,dx^*dH \\ &= a\epsilon \int F(X)\,dX = a\epsilon \end{aligned}$$

from the Corollary to Lemma 14 of [4(e)]. This proves that

$$\lim_{H \to 0} \phi_{\tilde{F}}(H;\partial(\pi)) = a\epsilon c_i' \qquad (H \in \mathfrak{h}_{(i)}).$$

But since $\bar{F}(0) = 1$, this implies that $c_i = a\epsilon c_i'$, and therefore $c_1 + \cdots + c_q = a\epsilon(c_1' + \cdots + c_q') \neq 0$.

6. Appendix. Let $\mathfrak{z}_0$ be a subalgebra of $\mathfrak{g}_0$ and Ξ_0 the analytic subgroup of G corresponding to $\mathfrak{z}_0$. We assume that $\mathfrak{z}_0$ is reductive in $\mathfrak{g}_0$. Let Ξ' be the normalizer of $\mathfrak{z}_0$ in G.

LEMMA 15. *Suppose* rank $\mathfrak{z}_0$ = rank $\mathfrak{g}_0$. *Then the factor group* Ξ'/Ξ_0 *is finite.*

Since $\mathfrak{z}_0$ is reductive, we can select (see the Corollary to Lemma 2 of [4(c)]) a finite number of Cartan subalgebras $\mathfrak{h}_1, \cdots, \mathfrak{h}_r$ of $\mathfrak{z}_0$ such that every Cartan subalgebra of $\mathfrak{z}_0$ is of the form $x\mathfrak{h}_i$ for some $x \in \Xi_0$ and some i $(1 \leqq i \leqq r)$. Suppose $\mathfrak{h}_1$ is conjugate to $\mathfrak{h}_i$ $(1 \leqq i \leqq k)$ under Ξ' but not to $\mathfrak{h}_i$ $(k < i \leqq r)$. Select $\xi_i \in \Xi'$ such that $\xi_i\mathfrak{h}_1 = \mathfrak{h}_i$ $1 \leqq i \leqq k$ $(\xi_1 = 1)$. Now let $x \in \Xi'$. Then it is clear that $x\mathfrak{h}_1 = y\mathfrak{h}_i = y\xi_i\mathfrak{h}_1$ for some $y \in \Xi_0$ and some i $(1 \leqq i \leqq k)$. Since $\operatorname{rank} \mathfrak{z}_0 = \operatorname{rank} \mathfrak{g}_0$ and $\mathfrak{z}_0$ is reductive in $\mathfrak{g}_0$, $\mathfrak{h}_1$ is also a Cartan subalgebra of $\mathfrak{g}_0$. Let A' be the normalizer of $\mathfrak{h}_1$ in G and A the Cartan subgroup of G corresponding to $\mathfrak{h}_1$. Then A'/A is a finite group (see [4(c), Lemma 10]). On the other hand, if A_0 is the analytic subgroup of G corresponding to $\mathfrak{h}_1$, $A \cap \Xi_0 \supset A_0$. Moreover, from Lemma 7 of [4(e)], A/A_0 is both compact and discrete and hence finite. This proves that $(A' \cap \Xi')/A_0$ is a finite group. Select elements $a_j \in A' \cap \Xi'$ such that $A' \cap \Xi'$ is the union of $a_j A_0$ $(1 \leqq j \leqq N)$. Then it is clear that $x^{-1} y \xi_i \in a_j A_0$ for some j, and therefore $x \in y \xi_i A_0 a_j^{-1} \subset \xi_i a_j^{-1} \Xi_0$ since Ξ_0 is obviously normal in Ξ'. This shows that the order of the group Ξ'/Ξ_0 cannot exceed rN.

Let $\mathfrak{l}$ be the semisimple Lie algebra of dimension 3 spanned over by the three elements H, X, Y which satisfy the relations $[H,X] = 2X$, $[H,Y] = -2Y$, $[X,Y] = H$. Let Ω denote the Casimir polynomial of $\mathfrak{l}$. Then

$$\Omega(tH + xX + yY) = 8(t^2 + xy) \qquad (t, x, y \in C).$$

Moreover, $\mathfrak{h} = CH$ is a Cartan subalgebra of $\mathfrak{l}$ and there are only two roots α and $-\alpha$ given by $\alpha(H) = 2H$. We take α as the positive root. Then Ω coincides with $2\alpha^2$ on $\mathfrak{h}$. Hence an element $Z \in \mathfrak{l}$ is regular if and only if $\Omega(Z) \neq 0$. Let $\mathfrak{l}'$ denote the set of regular elements in $\mathfrak{l}$.

Consider the automorphism ν of $\mathfrak{l}$ given by[2]

$$\nu = \exp\{-(-1)^{\frac{1}{2}}(\pi/4)\operatorname{ad}(X+Y)\}.$$

A simple calculation shows that $\nu(H) = (-1)^{\frac{1}{2}}(X-Y)$, $\nu(X-Y) = (-1)^{\frac{1}{2}}H$ and $\nu(X+Y) = X+Y$. Therefore $RH + RX + RY$ and $\nu(RH + RX + RY) = R(-1)^{\frac{1}{2}}H + R(-1)^{\frac{1}{2}}(X-Y) + R(X+Y)$ are two isomorphic real forms of $\mathfrak{l}$. Since $\Omega(H) = 8 > 0$, they are not compact. On the other hand $R(-1)^{\frac{1}{2}}H + R(X-Y) + R(-1)^{\frac{1}{2}}(X+Y)$ is also a real form of $\mathfrak{l}$ which is compact since Ω is negative definite on it. We shall denote by $\mathfrak{l}_0$ either one of the two[6] real forms $RH + RX + RY$ and $R(-1)^{\frac{1}{2}}H + R(X-Y) + R(-1)^{\frac{1}{2}}(X+Y)$. Put $\mathfrak{l}_0' = \mathfrak{l}' \cap \mathfrak{l}_0$. If $\mathfrak{l}_0$ is compact, zero is the only singular point in $\mathfrak{l}_0$, and therefore $\mathfrak{l}_0'$ is connected. On the other hand, if $\mathfrak{l}_0$ is noncompact, the singular set of $\mathfrak{l}_0$ consists of all points $tH + xX + yY$ $(t, x, y \in R)$ satisfying the equation $t^2 + xy = 0$. In this case $\mathfrak{l}_0'$ has three connected components $\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3$ given as follows:

$$\mathfrak{l}_1 \colon t^2 + xy > 0; \quad \mathfrak{l}_2 \colon t^2 + xy < 0, x > y; \quad \mathfrak{l}_3 \colon t^2 + xy < 0, x < y.$$

Notice that $H \in \mathfrak{l}_1$ and $X - Y \in \mathfrak{l}_2$. Let U be a neighborhood of zero in $\mathfrak{l}_0$.

---

[6] It is not difficult to see that apart from isomorphism these are the only two real forms of $\mathfrak{l}$. However, we do not need this fact.

We assume that $tZ \in U$ $(0 \leqq t \leqq 1)$ whenever $Z \in U$. Then it is obvious that $U \cap \mathfrak{l}_0'$ is connected if $\mathfrak{l}_0$ is compact and consists of three connected components $U \cap \mathfrak{l}_i$ $(i = 1, 2, 3)$ if $\mathfrak{l}_0$ is not compact.

From now on we consider only the noncompact case. The mapping $(tH + xX + yY) \to \begin{pmatrix} t & x \\ y & -t \end{pmatrix}$ $(t, x, y \in C)$ is an isomorphism of $\mathfrak{l}$ onto the Lie algebra of all 2×2 complex matrices with trace zero and we may identify the two under this isomorphism. Then $\mathfrak{l}_0$ becomes the real subalgebra of $\mathfrak{l}$ consisting of the real matrices. It is clear that $\Omega(Z) = -8 \det Z$ and the two eigenvalues of Z are $\pm(-\det Z)^{\frac{1}{2}}$ $(Z \in \mathfrak{l})$. Call an element $Z \in \mathfrak{l}_0'$ hyperbolic or elliptic according as these eigenvalues are real or pure imaginary. Then $\mathfrak{l}_1$ consists of hyperbolic and $\mathfrak{l}_2 \cup \mathfrak{l}_3$ of elliptic elements. Let L be the (connected) adjoint group of $\mathfrak{l}_0$. It is easily seen that every hyperbolic element is conjugate under L to tH for some real $t \neq 0$. Moreover, since $\exp \frac{\pi}{2} \operatorname{ad}(X - Y)$ maps H into $-H$, we can always assume that $t > 0$. Let R^+ and R^- be the set of all positive and negative real numbers, respectively, and put $R' = R^+ \cup R^-$. Then we prove similarly that every element in $\mathfrak{l}_2$ and $\mathfrak{l}_3$, respectively, is conjugate to $\theta(X - Y)$ for some θ in R^+ and R^-. It is easy to check that there exists no element $x \in L$ such that $x(X - Y) = -(X - Y)$.

Let dZ denote the Euclidean measure on $\mathfrak{l}_0$ given by[2] $dZ = (2\pi)^{-1} dt\,dx\,dy$, where $Z = tH + xX + yY$ $(t, x, y \in R)$. Consider the one parameter subgroup K in L corresponding to $(X - Y)$. Then K is compact. Let dk denote the normalized Haar measure on K so that $\int_K dk = 1$.

LEMMA 16. *For any* $f \in C_c(\mathfrak{l}_0)$ *put*

$$\Phi_f(t) = \int_{-\infty}^{\infty} \bar{f}(tH + xX)\,dx \qquad (t \in R^+)$$

$$\Psi_f(\theta) = |\theta| \int_0^{\infty} \bar{f}(\theta(e^t X - e^{-t} Y))(e^t - e^{-t})\,dt \qquad (\theta \in R'),$$

where $\bar{f}(Z) = \int f(kZ)\,dk$ $(Z \in \mathfrak{l}_0)$. *Then*

$$\int_{\mathfrak{l}_1} f(Z)\,dZ = \int_0^{\infty} t\Phi_f(t)\,dt$$

$$\int_{\mathfrak{l}_2} f(Z)\,dZ = \int_0^{\infty} \theta\Psi_f(\theta)\,d\theta, \qquad \int_{\mathfrak{l}_3} f(Z)\,dZ = \int_{-\infty}^{0} |\theta|\,\Psi_f(\theta)\,d\theta.$$

Since f vanishes outside a compact set, it is seen without difficulty that Φ_f and Ψ_f are well defined. Put $k_\theta = \exp\{\theta \operatorname{ad}(X - Y)\}$ $(\theta \in R)$ and consider the mapping $(\theta, t, x) \to (t', x', y')$ given by

$$k_\theta(tH + xX) = t'H + x'X + y'Y,$$

where $0 \leqq \theta < \pi$, $t > 0$ and $x \in R$. It follows from general considerations (see [4(a), Lemma 9]) that

$$|\partial(t', x', y')/\partial(\theta, t, x)| = ct,$$

where c is a constant. To obtain its value we compute the Jacobian at $\theta = 0$. Now

$$\{(\partial/\partial\theta) k_\theta(tH + xX)\}_{\theta=0} = [X - Y, tH + xX] = xH - 2tX - 2tY.$$

Hence

$$\left\{\frac{\partial(t', x', y')}{\partial(\theta, t, x)}\right\}_{\theta=0} = \det\begin{pmatrix} x & -2t & -2t \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = -2t.$$

Therefore $c = 2$. Let A, N be the one-parameter subgroups of L corresponding to H and X, respectively. Then we know from general considerations (see Iwasawa [5]) that $L = KNA$. Therefore every element in $\mathfrak{l}_1$ can be written in the form $t(knH)$ $(k \in K, n \in N, t \in R^+)$. Since $k_\pi = 1$, it follows that every point of $\mathfrak{l}_1$ is obtained under our mapping $(\theta, t, x) \to k_\theta(tH + xX)$. Moreover, a direct computation shows that this mapping is univalent. Hence

$$\int_{\mathfrak{l}_1} f(Z)\,dZ = 2(2\pi)^{-1} \int_0^\pi d\theta \int_0^\infty t\,dt \int_{-\infty}^\infty f(k_\theta(tH + xX))\,dx$$
$$= \int_0^\infty t\,dt \int_{-\infty}^\infty \bar{f}(tH + xX)\,dx = \int_0^\infty t\Phi_f(t)\,dt.$$

Moreover, if $L^* = L/A$ and dx^* is the invariant measure on L^*, it follows from the Corollary to Lemma 15 of [4(e)] that

$$\Phi_f(t) = t\int_{L^*} f(tx^*H)\,dx^* \qquad (f \in C_c(\mathfrak{l}_0),\ t \in R^+)$$

provided dx^* is suitably normalized.

Now put $a_t = \exp\{t \operatorname{ad} H\}$ $(t \in R)$ and consider the mapping $(\phi, t, \theta) \to (t', x', y')$ given by

$$k_\phi a_t(\theta(X - Y)) = t'H + x'X + y'Y$$

$(0 \leqq \phi < \pi, t \in R^+, \theta \in R')$. Then again it follows by general considerations[7] (or by actual computation) that

$$|\partial(t', x', y')/\partial(\phi, t, \theta)| = c\theta^2(e^{2t} - e^{-2t}),$$

where c is a constant. In order to obtain c we evaluate the left side at $\phi = 0$. Then $\theta a_t(X - Y) = \theta(e^{2t}X - e^{-2t}Y)$. Hence

$$[(\partial/\partial\phi)\{k_\phi a_t(\theta(X - Y))\}]_{\phi=0} = \theta[X - Y, e^{2t}X - e^{-2t}Y] = \theta(e^{2t} - e^{-2t})H.$$

Therefore

$$\left\{\frac{\partial(t', x', y')}{\partial(\phi, t, \theta)}\right\}_{\phi=0} = \det\begin{pmatrix} \theta(e^{2t} - e^{-2t}) & 0 & 0 \\ 0 & 2\theta e^{2t} & 2\theta e^{-2t} \\ 0 & e^{2t} & -e^{-2t} \end{pmatrix}$$

$= -4\theta^2(e^{2t} - e^{-2t})$, and so $c = 4$. A_+ be the set of all a_t with $t \geqq 0$. It is easy to see that $L = KA_+K$. Therefore every element in $\mathfrak{l}_2(\mathfrak{l}_3)$ can be written in the form $k_\phi a_t(\theta(X - Y))$ with $0 \leqq \phi < \pi$, $t \geqq 0$, $\theta \in R^+$ ($\theta \in R^-$ respectively). Moreover, if $t \neq 0$, this can be done only in one way since the normalizer of $R(X - Y)$ in L is exactly K. Hence

$$\int_{\mathfrak{l}_2} f(Z)\,dZ = 4(2\pi)^{-1}\int_0^\pi d\phi \int_0^\infty \theta^2 d\theta \int_0^\infty f(k_\phi a_t(\theta(X - Y)))(e^{2t} - e^{-2t})\,dt$$
$$= \int_0^\infty \theta\Psi_f(\theta)\,d\theta.$$

Similarly,

$$\int_{\mathfrak{l}_3} f(Z)\,dZ = 4(2\pi)^{-1}\int_0^\pi d\phi \int_0^\infty \theta^2 d\theta \int_0^\infty f(k_\phi a_t(-\theta(X - Y)))(e^{2t} - e^{-2t})\,dt$$
$$= \int_{-\infty}^0 |\theta|\,\Psi_f(\theta)\,d\theta.$$

On the other hand, if dz is the Haar measure on L, it follows from [4(b), Lemma 38] that

$$\Psi_f(\theta) = |\theta| \int_L f(\theta z(X - Y))\,dz \qquad (f \in C_c(\mathfrak{l}_0))$$

if dz is suitably normalized.

Now suppose $f \in C_c^\infty(\mathfrak{l}_0)$. Then we can conclude from Theorem 3 of [4(e)] that $\Phi_f \in \mathscr{C}(R^+)$ and $\Psi_f \in \mathscr{C}(R')$.

---

[7] See [4(a), p. 501] and Lemma 38 of [4(b)].

LEMMA 17. *Let f be a function in $C_c^\infty(\mathrm{I}_0)$. Then*

$$\Phi_{\partial(\Omega)f}(t) = \tfrac{1}{8}\, d^2\Phi_f(t)/dt^2 \qquad (t \in R^+)$$

$$\Psi_{\partial(\Omega)f}(t) = -\tfrac{1}{8}\, d^2\Psi_f(\theta)/d\theta^2 \qquad (\theta \in R').$$

Since $\Omega(H) = 8$ and $\Omega(X - Y) = -8$, this is an immediate consequence of Theorem 3 of [4(e)].

Put $\Phi_f(0) = \lim_{t\to 0} \Phi_f(t)$ $(t \in R^+)$, $\Psi_f^+(0) = \lim_{\theta\to 0} \Psi_f(\theta)$ $(\theta \in R^+)$ and $\Psi_f^-(0) = \lim_{\theta\to 0} \Psi_f(\theta)$ $(\theta \in R^-)$ for $f \in C_c^\infty(\mathrm{I}_0)$. (We know from Lemma 25 of [4(e)] that all these limits exist). Then it is obvious that $\Phi_f(0) = \int_{-\infty}^{\infty} \bar{f}(xX)\,dx$. So now let us consider $\Psi_f^+(0)$. It is obvious that

$$\lim_{\theta\to 0} \theta \int_0^\infty \bar{f}(\theta(e^tX - e^{-t}Y))\,e^{-t}\,dt = 0.$$

On the other hand, if $\theta \in R^+$,

$$\theta \int_0^\infty \bar{f}(\theta(e^tX - e^{-t}Y))\,e^{t}\,dt = \int_\theta^\infty \bar{f}(tX - \theta^2 t^{-1}Y)\,dt.$$

Moreover, if M is an upper bound for $|\partial(Y)\bar{f}|$, it is clear that $|\bar{f}(tX + sY) - \bar{f}(tX)| \leqq |s|\,M$ $(s \in R)$, and since $\bar{f}$ vanishes outside a compact set, we can select $T \in R^+$ such that $\bar{f}(tX + sY) = 0$ for all $s \in R$ if $t \geqq T$. Then if $\theta < T$, it follows that

$$\int_\theta^\infty |\bar{f}(tX - \theta^2 t^{-1}Y) - \bar{f}(tX)|\,dt \leqq \theta^2 \int_\theta^T M t^{-1}\,dt = M\theta^2 \log(T/\theta).$$

Hence

$$\lim_{\theta\to 0} \int_0^\infty \bar{f}(tX - \theta^2 t^{-1}Y)\,dt = \int_0^\infty \bar{f}(tX)\,dt \qquad (\theta \in R^+).$$

This proves that $\Psi_f^+(0) = \int_0^\infty \bar{f}(tX)\,dt$. Similarly one shows that $\Psi_f^-(0) = \int_{-\infty}^0 \bar{f}(tX)\,dt$. Thus we have obtained the following result.

LEMMA 18. *For any $f \in C_c^\infty(\mathrm{I}_0)$,*

$$\Phi_f(0) = \int_{-\infty}^{\infty} \bar{f}(tX)\,dt, \quad \Psi_f^+(0) = \int_0^\infty \bar{f}(tX)\,dt, \quad \Psi_f^-(0) = \int_{-\infty}^0 \bar{f}(tX)\,dt.$$

COROLLARY. *Put $f_m = \partial(\Omega^m)(\Omega^m f)$ $(f \in C_c^\infty(\mathrm{I}_0), m \geqq 0)$. Then*

$$\Phi_{f_m}(0) = c_m\Phi_f(0), \quad \Psi_{f_m}^+(0) = c_m\Psi_f^+(0), \quad \Psi_{f_m}^-(0) = c_m\Psi_f^-(0),$$

where $c_m = 4^m m!\,\Gamma(m + \tfrac{1}{2})/\Gamma(\tfrac{1}{2})$.

It is obvious that the differential operator $\partial(\Omega''') \circ \Omega'''$ is invariant under L and therefore also under K. Moreover $\Omega(X) = 0$. Hence our assertion is an immediate consequence of the Corollary to Lemma 19 of [4(d)].

Let U be an open neighborhood of zero in $\mathfrak{l}_0$.

LEMMA 19. *Suppose c_1, c_2, c_3 are three constants and*

$$c_1\Phi_f(0) = c_2\Psi_f^+(0) + c_3\Psi_f^-(0)$$

for all $f \in C_c^\infty(U)$. Then $c_1 = c_2 = c_3$.

Let $\mathfrak{l}^+$ be the set of all points of the form $tH + xX + yY$ $(t, y \in R; x \in R^+)$. We can obviously choose a positive number x_0 and a real-valued nonnegative function $f \in C_c^\infty(U \cap \mathfrak{l}^+)$ such that $f(x_0X) = 1$. A simple calculation shows that

$$k_\theta X = (\cos\theta \sin\theta)H + (\cos\theta)^2X - (\sin\theta)^2Y \qquad (\theta \in R).$$

Hence it is clear from Lemma 18 that $\Phi_f(0) = \Psi_f^+(0) > 0$ while $\Psi_f^-(0) = 0$. Therefore it follows from our hypothesis that $c_1 = c_2$. Similarly we prove that $c_1 = c_3$.

Let E be a vector space over R of dimension n and let $d\mu$ denote the Euclidean measure on E.

LEMMA 20. *Let U be a nonempty open set in E and $p_1, \cdots, p_r$ a finite number of continuous functions on U. Suppose $p_1, \cdots, p_r$ are linearly independent over C. Then we can select a function $f \in C_c^\infty(U)$ such that*

$$\int_U fp_i\, d\mu = \begin{cases} 1 \text{ if } i = 1, \\ 0 \text{ if } i \neq 1 \end{cases} \qquad (1 \leqq i \leqq r).$$

Let τ_i denote the distribution on U given by

$$\tau_i(g) = \int_U gp_i\, d\mu \qquad (g \in C_c^\infty(U)).$$

Let V be a vector space over C of dimension r and let $v_1, \cdots, v_r$ be a base for V. For any $g \in C_c^\infty(U)$, put $\tau(g) = \sum_{1 \leqq i \leqq r} \tau_i(g)v_i$ and let V_1 be the subspace of V consisting of all elements of the form $\tau(g)$. We claim $V_1 = V$. For otherwise, we could select a linear function $\lambda \neq 0$ on V such that $\lambda(\tau(g)) = 0$ for all $g \in C_c^\infty(U)$. Put $\lambda_i = \lambda(v_i)$ $1 \leqq i \leqq r$. Then not every λ_i is zero and

$$\lambda(\tau(g)) = \sum_{1 \leqq i \leqq r} \lambda_i\tau_i(g) = 0 \qquad (g \in C_c^\infty(U)).$$

Let $p=\sum_{1\leqq i\leqq r}\lambda_i p_i$. Since p_i are linearly independent, $p\neq 0$, and therefore it is obvious that $\int pg\,d\mu\neq 0$ for some $g\in C_c^\infty(U)$. However

$$\int pg\,d\mu=\sum_{1\leqq i\leqq r}\lambda_i\tau_i(g)=\lambda(\tau(g))=0,$$

and so we get a contradiction. This proves that $V_1=V$, and therefore we can choose $f\in C_c^\infty(U)$ such that $\tau(f)=v_1$. Then obviously f fulfills the desired condition.

INSTITUTE FOR ADVANCED STUDY,
COLUMBIA UNIVERSITY.

REFERENCES.

[1] E. Cartan, *Ann. Ecole Norm. Sup.*, vol. 44 (1927), pp. 345-467.

[2] C. Chevalley, *Theory of Lie groups*, Princeton University Press, 1946.

[3] L. Garding, *Math. Scand.*, vol. 1 (1953), pp. 55-72.

[4] Harish-Chandra, (a) *Trans. Amer. Math. Soc.*, vol. 76 (1954), pp. 485-528.
(b) *Amer. Jour. Math.*, vol. 78 (1956), pp. 564-628.
(c) *Trans. Amer. Math. Soc.*, vol. 83 (1956), pp. 98-163.
(d) *Amer. Jour. Math.*, vol. 79 (1957), pp. 87-120.
(e) *Amer. Jour. Math.*, vol. 79 (1957), pp. 193-257.
(f) *Proc. Nat. Acad. Sci. U. S. A.*, vol. 42 (1956), pp. 538-540.

[5] K. Iwasawa, *Ann. of Math.*, vol. 50 (1949), pp. 507-557.

[6] F. John, *Proceedings of the symposium on spectral theory and differential problems*, Stillwater, Okla., (1951), pp. 113-175.

[7] L. Schwartz, *Théorie des distributions I*, Paris, Hermann, 1950.

[8] A. Weil, *L'intégration dans les groupes topologiques et ses applications*, Paris, Hermann, 1940.

LOCAL CHARACTERIZATION OF INTEGRAL QUADRATIC FORMS BY GAUSS SUMS.*

By O. T. O'Meara.

This paper is concerned with the existence of a solution X to the $n \times n$ matrix equation $X^THX = G$, with H and G symmetric. When the coefficient field has characteristic $\neq 2$, this is the same as determining the equivalence class of a quadratic form. Invariants for the equivalence class of H under the transformation X^THX have been given over certain arithmetical fields and a discussion of these results can be found, for instance, in Witt's work on quadratic forms [11]. The problem of finding when there is a unimodular solution X has been solved over local fields by Durfee, Jones, Minkowski and the author. As far as the known results go, the general solution to this problem is in terms of Hasse symbols. There is another characterization due to Minkowski which involves Gauss sums but, to use the language of valuation theory, this has been proved over the p-adic numbers only. We shall extend this result to local fields with finite residue class field.

There are three levels of difficulty in the local theory and they are determined by the way in which 2 splits in the coefficient field. Thus we shall find that the Gauss sums alone characterize the integral equivalence class of H when $\operatorname{ord} 2 = 0$, while one must include the type as an invariant in the unramified case. This much is in agreement with the rational p-adic results of Minkowski. In the ramified theory further conditions must be imposed and these will be given in terms of the invariants a_j, $v(j)$ introduced in [8]; however, we shall see that the Gauss sums alone form a complete set of invariants for a unitary H over any of these fields.

1. Group characters.

We consider a local field F with ring of integers $\mathfrak{o}$ and prime ideal $\pi\mathfrak{o}$. We assume that the residue class field $\mathfrak{o}/(\pi\mathfrak{o})$ is finite of characteristic 2, while F itself has characteristic 0. Thus the number of elements in $\mathfrak{o}/(\pi\mathfrak{o})$ is of the form 2^f. Define the ramification index e by the relation $e = \operatorname{ord} 2$; under these restrictions we see that $1 \leqq e < \infty$. It follows [1] from these assumptions that F must be a finite extension of the 2-adic numbers, the degree of the extension being ef. The $\mathfrak{o}$-ideal $\mathfrak{o}(r)$ is

---

* Received December 4, 1956.

defined by $\mathfrak{o}(r) = \pi^r\mathfrak{o}$ for $r \geqq 0$. If $q \geqq r$, then $\mathfrak{o}(q) \subseteq \mathfrak{o}(r)$. If $\alpha_1, \cdots$ is a complete set of representatives of $\mathfrak{o}/\mathfrak{o}(r)$ and if $\beta_1, \cdots$ is a complete set for $\mathfrak{o}/\mathfrak{o}(q-r)$, then it is easily seen that $\alpha_i + \pi^r\beta_j$ form a complete set for $\mathfrak{o}/\mathfrak{o}(q)$. We shall write $[\pi^t]$ to denote an element of ordinal t; $\{\pi^t\}$ will denote an element of ordinal $\geqq t$. The relation $\alpha \cong \beta$ means that there is a unit in $\mathfrak{o}$ whose square in α/β. If ϵ is a unit, then $\epsilon \cong 1 \bmod \pi$ since $\mathfrak{o}/(\pi\mathfrak{o})$ is a finite field. Consider the greatest value of k for which $\epsilon \cong 1 + [\pi^k]$. If $k > 2e$, then $k = \infty$ by Hensel's lemma. On the other hand,

$$k < 2e \Longrightarrow k \text{ odd}. \tag{1}$$

A mapping χ of $\mathfrak{o}$ into the multiplicative group of complex numbers is called a *character* if $\chi(\alpha + \beta) = \chi(\alpha)\chi(\beta)$ for all α, β in $\mathfrak{o}$, and if $\chi(\mathfrak{o}(r)) = 1$ for some $r < \infty$. Any ideal $\mathfrak{o}(r)$ for which $\chi(\mathfrak{o}(r)) = 1$ is called a *support* of χ; the largest ideal in $\mathfrak{o}$ which supports χ is called the *maximal support* of χ; $\mathfrak{o}(m(\chi))$, or simply $\mathfrak{o}(m)$, will be used to denote the maximal support of χ; then we have $0 \leqq m(\chi) < \infty$. For example, $m(\chi) = 0$ means that χ is the identity character taking the value 1 for all $\alpha \in \mathfrak{o}$. Note that $\chi(0) = 1$ for any χ.

We define the *character group* $\mathfrak{D}$ of $\mathfrak{o}$ as the set of all characters on $\mathfrak{o}$, the group structure being defined by

$$\chi\theta(\alpha) = \chi(\alpha)\theta(\alpha) \qquad \text{for all } \alpha \in \mathfrak{o};$$

the identity of $\mathfrak{D}$ is the identity character. If $\mathfrak{D}(r) \subseteq \mathfrak{D}$ consists of all $\chi \in \mathfrak{D}$ for which $\chi(\mathfrak{o}(r)) = 1$, then $\mathfrak{D}(r)$ is a subgroup of $\mathfrak{D}$. And any character $\chi \in \mathfrak{D}(r)$ can be interpreted as a character on $\mathfrak{o}/\mathfrak{o}(r)$ since χ is supported by $\mathfrak{o}(r)$. Conversely, every character on $\mathfrak{o}/\mathfrak{o}(r)$ can be interpreted as a character in $\mathfrak{D}(r)$. Since $\mathfrak{o}/\mathfrak{o}(r)$ is a finite abelian group of order 2^{fr}, it follows from the theory of characters [1] that $\mathfrak{D}(r)$ contains 2^{fr} elements. We have the reverse order relations

$$\mathfrak{o} = \mathfrak{o}(0) \supset \mathfrak{o}(1) \cdots \supset \mathfrak{o}(r) \supset \mathfrak{o}(r+1) \cdots \supset 0,$$

$$1 = \mathfrak{D}(0) \subset \mathfrak{D}(1) \cdots \subset \mathfrak{D}(r) \subset \mathfrak{D}(r+1) \cdots \subset \mathfrak{D}.$$

From the theory of characters on a finite abelian group [10] we get

$$\sum_{\alpha \bmod \mathfrak{o}(r)} \chi(\alpha) = \begin{cases} 0 & \text{if } \chi \neq 1,\ \chi \in \mathfrak{D}(r) \\ 2^{fr} & \text{if } \chi = 1. \end{cases} \tag{2}$$

Consider a character χ with maximal support $\mathfrak{o}(m)$. For fixed integers A and B define

$$\theta(\alpha) = \chi(A\alpha), \qquad \psi(\alpha) = \chi(B\alpha) \qquad \text{for all } \alpha \in \mathfrak{o}.$$

Then $\theta \in \mathfrak{O}(m)$, $\psi \in \mathfrak{O}(m)$. It is easy to see that

$$\theta = \psi \Leftrightarrow A \equiv B \bmod \mathfrak{o}(m).$$

Thus 2^{fm} characters can be obtained by allowing A to vary through $\mathfrak{o}$; in other words, we then get all $\mathfrak{O}(m)$. If $A = E\pi^k$ $(0 \leqq k \leqq m)$ and if E is allowed to vary through all units $\bmod \pi^{m-k}$, the dependent variable θ ranges through all those characters with maximal support $\mathfrak{o}(m-k)$. We define $\chi_{(k)}$ as the character given by

$$\chi_{(k)}(\alpha) = \chi(\pi^k \alpha) \qquad \text{for all } \alpha \in \mathfrak{o}. \tag{3}$$

Now let θ be any character with maximal support $\mathfrak{o}(m-k)$; then $\theta(\alpha) = \chi(\pi^k E\alpha)$ for some fixed unit E; so putting $\psi(\alpha) = \chi(E\alpha)$ we see that $\psi_{(k)}(\alpha) = \psi(\pi^k\alpha) = \theta(\alpha)$ for all $\alpha \in \mathfrak{o}$. So we have proved that *every* θ *with maximal support* $\mathfrak{o}(m-k)$ *is a* $\psi_{(k)}$ *for some* ψ *with maximal support* $\mathfrak{o}(m)$. We shall need the dual of (2):

$$\sum_{\chi \in \mathfrak{O}(r)} \chi(\alpha) = \begin{cases} 0 & \text{if } \alpha \notin \mathfrak{o}(r) \\ 2^{fr} & \text{if } \alpha \in \mathfrak{o}(r). \end{cases} \tag{4}$$

Remark. Our given local field must contain a replica of the 2-adic numbers Q_2; in fact assume that $Q_2 \subseteq F$. Any $A \in Q_2$ can be put in the form $A = \lambda 2^{-\mu} + A_1$, where λ, μ are rational integers and $|A_1| \leqq 1$. Define

$$\exp(2\pi i A) = \exp(2\pi i \lambda 2^{-\mu})$$

where π and i are the complex numbers usually denoted by these letters. It is easy to see that this is well-defined and that

$$\exp(2\pi i(A+B)) = \exp(2\pi i A)\exp(2\pi i B).$$

Now put

$$\theta_\omega(\alpha) = \exp(2\pi i T(\omega\alpha))$$

for $\omega \in F$, $\alpha \in \mathfrak{o}$, where T denotes the trace from F to Q_2. Then θ_ω is a character defined on $\mathfrak{o}$. Let $\mathfrak{d}$ be the different [1] of the extension F/Q_2. It is easily seen that all $\omega^{-1} \notin \mathfrak{d}$ give trivial characters θ_ω. So we can assume that $\omega^{-1} \in \mathfrak{d}$. Then θ_ω has maximal support $\omega^{-1}\mathfrak{d}^{-1}$. In particular, given any $\mathfrak{p} \subseteq \mathfrak{o}$, there is a θ_ω having $\mathfrak{p}$ as maximal support. Taking $\theta_{\epsilon\omega}$, $|\epsilon| = 1$, instead of θ_ω gives all characters with maximal support $\mathfrak{p}$. Thus every character of $\mathfrak{O}$ can be obtained as a θ_ω for some $\omega^{-1} \in \mathfrak{d}$.

2. The Gauss sums of a lattice. V denotes a non-degenerate n-dimensional vector space with scalar product $x \cdot y$; and L is a lattice on V. For a fixed $\alpha \in F$, denote by αL the set of vectors αz with $z \in L$; let $\alpha \circ V$ be the vector space V provided with the new metric $x \circ y = \alpha(x \cdot y)$; let $\alpha \circ L$ be the point set L in the space $\alpha \circ V$. It is assumed that $N(L) \subseteq \mathfrak{o}$; i.e., L *will be integral.* These concepts are defined in [8]; we use the same notation here as in the introduction of [8].

For $r \geqq 0$, put $L(r) = \pi^r L$; e.g., $L(0) = L$. Call $x_1, \cdots$ a complete set of representatives of L modulo π^r if

(i) $$x_i - x_j \in L(r) \Leftrightarrow x_i = x_j,$$

(ii) for each $x \in L$ there is an x_i such that $x - x_i \in L(r)$.

In effect, the x_i are any set of representative vectors of $L/L(r)$. If $y_1, \cdots$ is another complete set of representatives of L modulo π^r, then the y_i can be reordered in such a way that $x_i - y_i \in L(r)$. In particular, these two sets have the same number of elements. By expressing L in a minimal basis we see that any such set of representatives contains 2^{nfr} vectors. Now let $z_1, \cdots$ be a complete set for L modulo π^{q-r}, with $q \geqq r$. Then it is easy to prove that $x_i + \pi^r z_j$ is a complete set for L modulo π^q.

We define the *Gauss sum*

$$\chi(L;\pi^r) = \sum_{x \bmod L(r)} \chi(x^2) \qquad \text{for } \chi \in \mathfrak{D}(r). \tag{5}$$

For short, put

$$\chi(L) = \chi(L;\pi^{m(\chi)}). \tag{6}$$

The definitions are independent of the choice of representatives of $L/L(r)$.

PROPOSITION 1. *If $L = J \oplus K$, then $\chi(L) = \chi(J)\chi(K)$.*

Proof. $$\chi(L) = \Sigma\Sigma\chi((x+y)^2) = \Sigma\Sigma\chi(x^2+y^2) = \Sigma\Sigma\chi(x^2)\chi(y^2)$$
$$= \Sigma\chi(x^2)\Sigma\chi(y^2) = \chi(J)\chi(K),$$

with $x \bmod J(m)$, $y \bmod K(m)$. q.e.d.

PROPOSITION 2. $\chi(L;\pi^r) = 2^{nf(r-m(\chi))}\chi(L)$.

Proof. $$\chi(L;\pi^r) = \Sigma\Sigma\chi((x+\pi^m y)^2) = \Sigma\Sigma\chi(x^2 + 2\pi^m x \cdot y + \pi^{2m}y^2)$$
$$= \Sigma\chi(\pi^{2m}y^2)\Sigma\chi(x^2) = 2^{fn(r-m)}\chi(L)$$

with $x \bmod L(m)$ and $y \bmod L(r-m)$. q.e.d.

For $r \geqq 0$, let the *representation number* $L(h;\pi^r)$ be defined as the number of times $h \in \mathfrak{o}$ is represented modulo π^r by a complete set of representative vectors of $L/L(r)$. This quantity is well-defined.

PROPOSITION 3. *L and K have the same dimension. Then $\chi(L) = \chi(K)$ for all $\chi \in \mathfrak{D}(r)$ if and only if $L(h;\pi^r) = K(h;\pi^r)$ for all $h \in \mathfrak{o}$.*

Proof. Put $\dim L = n = \dim K$. The condition $\chi(L) = \chi(K)$ can be replaced by $\chi(L;\pi^r) = \chi(K;\pi^r)$ in virtue of Proposition 2. In general we have

$$\chi(L;\pi^r) = \sum_{h \bmod \mathfrak{o}(r)} L(h;\pi^r)\chi(h). \tag{7}$$

In particular, this proves the sufficiency. We now prove the necessity.

For a fixed h_0, (7) implies that

$$\chi^{-1}(h_0)\chi(L;\pi^r) = \sum L(h;\pi^r)\chi(h-h_0) + L(h_0;\pi^r),$$

where the summation extends over $h \bmod \mathfrak{o}(r)$, $h \not\equiv h_0 \bmod \mathfrak{o}(r)$. Now summing both sides of this equation over $\chi \in \mathfrak{D}(r)$, we see that (4) implies

$$2^{fr}L(h_0;\pi^r) = \sum_{\chi \in \mathfrak{D}(r)} \chi^{-1}(h_0)\chi(L;\pi^r).$$

This also holds for K. Hence $L(h_0;\pi^r) = K(h_0;\pi^r)$. q. e. d.

Let L be an integral lattice and consider $\pi^k \circ L$ with k a non-negative integer. It is easy to see that

$$\chi(\pi^k \circ L;\pi^r) = \chi_{(k)}(L;\pi^r) \qquad \text{if } \chi \in \mathfrak{D}(r). \tag{8}$$

For all $\chi \in \mathfrak{D}$ we therefore have

$$\begin{aligned} \chi(\pi^k \circ L) &= 2^{nfk}\chi_{(k)}(L) && \text{if } 0 \leqq k \leqq m(\chi), \\ \chi(\pi^k \circ L) &= 2^{nfm(\chi)} && \text{if } m(\chi) \leqq k. \end{aligned} \tag{9}$$

Now consider $\chi \in \mathfrak{D}(r+k)$ with $r \geqq 0$, $k \geqq 0$ fixed; let L and K be n-dimensional integral lattices. Then it follows from (9) that

$$\chi(\pi^k \circ L) = \chi(\pi^k \circ K) \Leftrightarrow \chi_{(k)}(L) = \chi_{(k)}(K). \tag{10}$$

If $\theta \in \mathfrak{D}(r)$, then $\theta = \chi_{(k)}$ for some $\chi \in \mathfrak{D}(r+k)$. So *$L$ and K have the same Gauss sums modulo π^r if and only if $\pi^k \circ L$ and $\pi^k \circ K$ have the same Gauss sums modulo π^{r+k}.*

3. Fundamental invariants of a lattice.

Let L and K be two lattices in the same space V. We put

$$L^2 = \{x^2 \mid x \in L\}, \qquad x_0 \cdot L = \{(x_0 \cdot x) \mid x \in L\},$$
$$L \cdot K = \{(x \cdot y) \mid x \in L \text{ and } y \in K\}.$$

Then $x_0 \cdot L$ and $L \cdot K$ are ideals; L^2 is not an ideal, but L^2 generates $N(L)$.

Thus $\alpha \in L^2$ means that L represents α; and $\alpha \in L^2 \bmod \pi^k$ means that $x^2 - \alpha \in \mathfrak{o}(k)$, for some $x \in L$. If $L_1 \oplus L_2 \oplus \cdots \oplus L_t$ is a canonical decomposition of L, we put $L_j \cdot L_j = \mathfrak{o}(s(j))$ and we define $N(L_{(s(j))}) = \mathfrak{o}(u(j))$ where $L_{(s(j))}$ is the invariant substructure given by

$$L_{(s(j))} = \{x \mid x \in L \text{ and } x \cdot L \subseteq \mathfrak{o}(s(j))\}.$$

Define $\mathfrak{o}(v(j)) = \Sigma x^2 \mathfrak{o} + 2\pi^{s(j)}\mathfrak{o}$ where $x \in L_{(s(j))}$ with $\operatorname{ord} x^2$ and $u(j)$ of opposite parity. Then for any $a_j \in L_{(s(j))}{}^2 \bmod \pi^{v(j)}$ with $\operatorname{ord} a_j = u(j)$, it is true that

$$L_{(s(j))}{}^2 \subseteq a_j \mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o}; \tag{11}$$

and $a_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o}$ is an additive group. If L is big, there is equality in (11). We shall call the quantities a_j and $v(j)$ the *fundamental invariants* of L. Then $v(j)$ is unique; while a_j is fixed modulo $\pi^{v(j)}$, but for a factor which is the square of a unit. Every lattice L has a *saturated decomposition* $L = \Sigma L_\lambda$ in which $N(L_j) = \mathfrak{o}(u(j))$, $1 \leqq j \leqq t$. If L is big, it has a *supersaturated decomposition* $L = \Sigma L_\lambda$ in which $L_j{}^2 = a_j\mathfrak{o}^2 + \pi^{v(j)}\mathfrak{o} = L_{(s(j))}{}^2$, for $1 \leqq j \leqq t$. For a detailed discussion, see Sections 1-4 of [8].

4. Unitary lattices. Throughout this section L and K will be n-dimensional π^0-unitary lattices with the same fundamental invariants $v_L = v = v_K$ and $a(L) \cong a \cong a(K) \bmod \pi^v$. We write $u = \operatorname{ord} a$; assume that $\pi^u\mathfrak{o} = a\mathfrak{o} = N(L) = N(K)$. Using results in [8] we shall characterize L in terms of its fundamental invariants and its Gauss sums.

Suppose that n is even and $d(L) \cong (-1)^{\frac{1}{2}n}(1 + [\pi^{u+v}])$. We contend that

$$L \cong \begin{pmatrix} [\pi^u] & 1 \\ 1 & [\pi^v] \end{pmatrix} \oplus \Sigma \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{12}$$

If $n = 2$ this follows by a determinantal consideration. So take $n \geqq 4$ and express L in the semi-canonical decomposition

$$L \cong \begin{pmatrix} [\pi^u] & 1 \\ 1 & \{\pi^v\} \end{pmatrix} \oplus \begin{pmatrix} \pi^v & 1 \\ 1 & \{4\pi^{-v}\} \end{pmatrix} \oplus \Sigma \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{13}$$

given in (12)-(14) of [8]. If u and v have the same parity, again we are through. So take $n \geqq 4$ with $u + v$ odd. Let the basis corresponding to (13) be $\langle x \rangle$. Then we can assume that $\operatorname{ord} x_2{}^2 = v$ since

$$d(L) \cong (-1)^{\frac{1}{2}n}(1 + [\pi^{u+v}]).$$

By successively applying $\operatorname{op}(x_3 \rightarrow x_3 + \alpha x_2)$ and $\operatorname{op}(x_3 \rightarrow x_3 + \alpha x_1)$ we get the desired result (12).

Now consider the $(n+2)$-dimensional lattices $J \oplus L$, $J \oplus K$ where

$$J \cong \begin{pmatrix} a & 1 \\ 1 & \pi^v \end{pmatrix}.$$

CONTENTION. *If* $\mathfrak{p}$ *is any ideal,* $0 \subseteq \mathfrak{p} \subseteq \mathfrak{o}(v)$, *then*

$$J \oplus L \cong J \oplus K \bmod \mathfrak{p} \Longrightarrow L \cong K \bmod \mathfrak{p}. \tag{14}$$

Proof. Clearly $J \oplus L$, L, K, $J \oplus K$ all have the same fundamental invariants. Then $J \oplus L$ and $J \oplus K$ satisfy the condition of Theorem 1 [8], hence L and K satisfy these conditions, hence $L \cong K \bmod \mathfrak{p}$. q. e. d.

Let H be a π^k-hyperbolic plane, $k \geqq 0$; let χ be any character in $\mathfrak{O}$. Then

$$\chi(H) = \sum_{\alpha \bmod \mathfrak{o}(m)} \sum_{\beta \bmod \mathfrak{o}(m)} \chi(2\pi^k \alpha\beta).$$

But $\chi(2\pi^k\alpha\beta) = \theta(\beta)$ is a character for each fixed α. Hence it follows from (2) that

$$\sum_{\beta \bmod \mathfrak{o}(m)} \chi(2\pi^k\alpha\beta) \geqq 0,$$

with strict inequality occurring for at least one value of α. Hence

$$\chi(H) > 0. \tag{15}$$

THEOREM 1. *L and K are π^0-unitary lattices of the same dimension such that $v_L = v = v_K$ and $a(L) \cong a \cong a(K) \bmod \pi^v$. If $0 \subseteq \mathfrak{p} \subseteq \pi^v \mathfrak{o}$, then $L \cong K \bmod \mathfrak{p}$ if and only if* (i) $d(L) \cong d(K) \bmod a\mathfrak{p}$, (ii) $\chi(L) = \chi(K)$ *for all χ supported by $\mathfrak{p}$.*

Proof. The necessity follows at once from Theorem 1 of [8]. We now prove the sufficiency.

If $|\mathfrak{p}| \geqq |4\pi^{-v}|$, we are through by Theorem 1 of [8]. Hence assume that $|\mathfrak{p}| < |4\pi^{-v}|$ for the rest of the proof. By Proposition 9 of [8] we can assume that L and K are big. Since both L and K now represent a, it suffices to prove that $(a) \oplus L \cong (a) \oplus K \bmod \mathfrak{p}$ when $u = 0$, in virtue of Corollary 9 of [8]. In other words, we can assume that n is even. We have $|a\mathfrak{p}| \leqq |4\pi^{u+1-v}| \leqq |\pi^{u+1+v}|$, and so $d(L) \cong d(K) \bmod \pi^{u+v+1}$. Thus we either have

$$d(L) \cong (-1)^{\frac{1}{2}n}(1 + [\pi^{u+v}]), \qquad d(K) \cong (-1)^{\frac{1}{2}n}(1 + [\pi^{u+v}]) \tag{16}$$

or

$$d(L) \cong (-1)^{\frac{1}{2}n}(1 + \{\pi^{u+v+1}\}), \qquad d(K) \cong (-1)^{\frac{1}{2}n}(1 + \{\pi^{u+v+1}\}). \tag{17}$$

In the latter case adjoin $\begin{pmatrix} a & 1 \\ 1 & \pi^v \end{pmatrix}$ to L and K; then the enlarged lattices satisfy (16); and it suffices to prove the isometry of the new lattices modulo $\mathfrak{p}$ by (14). In effect we can therefore assume that (16) holds for L and K. By (12) and (15) the problem reduces to the case $n = 2$. We assume that this is so.

Since L and K represent the same numbers modulo $\mathfrak{p}$ we can write

$$L \cong \begin{pmatrix} \epsilon\pi^u & 1 \\ 1 & \alpha\pi^v \end{pmatrix}, \qquad K \cong \begin{pmatrix} \epsilon\pi^u + \{\mathfrak{p}\} & 1 \\ 1 & \beta\pi^v \end{pmatrix}$$

with ϵ a unit, α and β integers. Define

$$K^* \cong \begin{pmatrix} \epsilon\pi^u & 1 \\ 1 & \beta\pi^v + \Gamma \end{pmatrix}$$

where Γ is chosen in $\mathfrak{p}$ so that $d(L) \cong d(K^*)$. Then $L \cong K^*$ by Theorem 14.3 of [7], hence $L \cong K \bmod \mathfrak{p}$. q. e. d.

Note. We use the Hasse symbol $S(L)$ in references to [8]. This is defined for the space V by Witt [11] and we put $S(L) = S(V)$. For the general laws obeyed by $S(L)$ see [11]. In addition we have seen in [8] that over fields of our type,

$$(1 + 4\alpha, \epsilon) = 1, \tag{18}$$

$$(1 + 4\alpha, \epsilon\pi) = 1 \Leftrightarrow (1 + 4\alpha)^{\frac{1}{2}} \in F, \tag{19}$$

where $\alpha \in \mathfrak{o}$ and $|\epsilon| = 1$. Also

$$(A, B) = (1 + 4C, \pi) \quad \text{for some } C \in \mathfrak{o}. \tag{20}$$

And since $\mathfrak{o}/(\pi\mathfrak{o})$ is a finite field it has a quadratic extension, hence there is a unit $E \in \mathfrak{o}$ such that

$$(1 + 4E)^{\frac{1}{2}} \notin F. \tag{21}$$

Now let L and K be π^0-unitary lattices of the same odd dimension such that $\chi(L) = \chi(K)$ for all $\chi \in \mathfrak{D}(2e + 1)$. We shall prove

$$d(L) \cong d(K). \tag{22}$$

Assume that this equation is false for given L and K. Put $L' \cong (1) \oplus (\pi \circ L)$ and $K' \cong (1) \oplus (\pi \circ K)$. Then $\chi(L') = \chi(K')$ for all $\chi \in \mathfrak{D}(2e + 2)$. Using the "op" transformations and the operator $\mathfrak{R}$ of [8], or otherwise, it is easily seen that

$$L' \cong [1] \oplus [\pi] \oplus \sum \begin{pmatrix} 0 & \pi \\ \pi & 0 \end{pmatrix}.$$

And similarly with K'. By (15) we can therefore assume that $L' \cong [1] \oplus [\pi]$

and $K' \cong [1] \oplus [\pi]$. By a suitable change of metric on L' and K', we can take $L' \cong 1 \oplus [\pi]$; by a suitable choice of prime π we can take $L' \cong 1 \oplus \pi$. Now $K'(1;4\pi^2) = L'(1;4\pi^2)$. By Hensel's lemma we therefore have

$$L' \cong 1 \oplus \pi, \qquad K' \cong 1 \oplus \pi(1 + G\pi^k) \tag{23}$$

where G is a unit and either (i) $k = 2e$, or (ii) $k < 2e$ with k odd. (i) Since $k = 2e$ with $(1 + G\pi^{2c})^{\frac{1}{2}} \notin F$, it is easily seen that $(1 + G\pi^{2e})\pi \notin (L')^2$, which is impossible since L' and K' represent the same numbers modulo $4\pi^2$. (ii) If $k < 2e$ with k odd, we choose a unit E for which $(1 + 4E)^{\frac{1}{2}} \notin F$. Then there is a unit α such that $\alpha^2 G \equiv E \bmod \pi$. Put $\epsilon = 1 + 4\alpha^2\pi^{-k}$. Then

$$\epsilon \in (L')^2, \qquad \epsilon(1 + 4E) \cong \epsilon + 4\alpha^2 G \in (K')^2.$$

But this implies that $\epsilon(1 + 4E) \in (L')^2$, which is impossible since $L' \cong \epsilon \oplus [\pi]$.

THEOREM 2. *L and K are π^0-unitary lattices of the same dimension. Then $L \cong K$ if and only if $\chi(L) = \chi(K)$ for all $\chi \in \mathfrak{D}(2e+1)$.*

Proof. Adjoin a π^0-unitary lattice to both L and K so that the enlarged lattices have odd dimension. Then the enlarged lattices have the same determinant by (22). Hence $d(L) \cong d(K)$.

Now $L^2 \equiv K^2 \bmod 4\pi$, hence L and K have the same fundamental invariants, hence $L \cong K \bmod 4\pi$ by Theorem 1, hence $L \cong K$ by Theorem 15.1 of [7]. This proves the sufficiency. The necessity is obvious. q. e. d.

5. The zeros of the Gauss sums. We have seen in (15) that the Gauss sums of a hyperbolic plane never vanish. Thus, for example, it follows that

$$\chi(J) \neq 0 \text{ if } J \cong \begin{pmatrix} 2 & 1 \\ 1 & \{2\} \end{pmatrix}, \tag{24}$$

since $J \oplus J$ is the orthogonal sum of two hyperbolic planes. In this section we solve for χ the equation

$$\chi(L) = 0, \qquad\qquad L \text{ fixed and unitary.} \tag{25}$$

LEMMA 1. *L is a π^0-unitary lattice with norm $\mathfrak{o}(u)$. The character χ has maximal support $\mathfrak{o}(m)$ where $0 \leqq m \leqq u$ or $m \geqq 2e - u$. Then $\chi(L) \neq 0$.*

Proof. If this is true for an enlargement of L it is true for L by Proposition 1. Hence assume $\dim L$ even. Since L is now an orthogonal sum of binary lattices of norm $\mathfrak{o}(u)$ it suffices to assume that L is binary, again by Proposition 1. Suppose

$$L \cong \begin{pmatrix} \epsilon\pi^u & 1 \\ 1 & \alpha\pi^v \end{pmatrix} \qquad \alpha \in \mathfrak{o} \tag{26}$$

where v is the second fundamental invariant of L. Using the "op" transformations of [8] we see that

$$\begin{pmatrix} \epsilon\pi^u & 1 \\ 1 & \alpha\pi^v \end{pmatrix} \oplus \begin{pmatrix} -\epsilon\pi^u & 1 \\ 1 & -\alpha\pi^v \end{pmatrix} \cong \begin{pmatrix} [\pi^u] & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} [\pi^u] & 1 \\ 1 & 0 \end{pmatrix}.$$

Hence the problem reduces to the case where L has the form (26) with $\alpha = 0$.

If $0 \leqq m \leqq u$, then L is a hyperbolic plane modulo $\mathfrak{o}(m)$ and so $\chi(L) \neq 0$ by (15). So assume that $m \geqq 2e - u$. Then

$$\chi(L) = \sum_{\alpha \bmod \mathfrak{o}(m)} \sum_{\beta \bmod \mathfrak{o}(m)} \chi(\epsilon\pi^u\alpha^2)\chi(2\alpha\beta). \tag{27}$$

Now

$$\chi(\epsilon\pi^u\alpha^2) \sum_{\beta \bmod \mathfrak{o}(m)} \chi(2\alpha\beta) = \begin{cases} 0 & \text{if } \alpha \notin \tfrac{1}{2}\mathfrak{o}(m) \\ 2^{fm} & \text{if } \alpha \in \tfrac{1}{2}\mathfrak{o}(m) \end{cases} \tag{28}$$

by (2). Hence $\chi(L) > 0$. q. e. d.

Consider the lattices

$$L \cong \begin{pmatrix} \epsilon\pi^u & 1 \\ 1 & 0 \end{pmatrix}, \quad K \cong \begin{pmatrix} \epsilon\pi^{u+k} & 1 \\ 1 & 0 \end{pmatrix}, \quad |\epsilon| = 1,\ u \geqq 0,\ k \geqq 0, \tag{29}$$

and the character χ with $m(\chi) = m = e + k$. Using (27) and (28) we see that

$$\chi(L) = \Sigma\Sigma\, \chi(\epsilon\pi^u\pi^{2k}\alpha^2)\,\chi(2\pi^k\alpha\beta) = 2^{kf}\, \Sigma\Sigma\, \chi_{(k)}(\epsilon\pi^{u+k}\alpha^2)\,\chi_{(k)}(2\alpha\gamma)$$

with $\alpha \bmod \mathfrak{o}(m-k)$, $\beta \bmod \mathfrak{o}(m)$, $\gamma \bmod \mathfrak{o}(m-k)$. Hence

$$\chi(L) = 2^{kf}\chi_{(k)}(K). \tag{30}$$

Lemma 2. *Let L have the form* (29) *with $u < m < 2e - u$. If $u + m$ is even, then* (i) *$\chi(L) \neq 0$ and* (ii) *$\chi(L) = 0$ have solutions with $m(\chi) = m$.* (iii) *If $u + m$ is odd, then $\chi(L) = 0$ for all χ with $m(\chi) = m$.*

Proof. (i) Suppose if possible that $\chi(L) = 0$ for all χ with $m(\chi) = m$. Define

$$J \cong \begin{pmatrix} \epsilon\pi^u & 1 \\ 1 & \pi^{m-1} \end{pmatrix}, \qquad H \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

In virtue of the isometry $J \oplus H \cong L \oplus \cdots$ we have $\chi(J) = 0$. Hence $\chi(J) = \chi(L)$ when $m(\chi) = m$. But $\chi(J) = \chi(L)$ when $\chi \in \mathfrak{D}(m-1) \subseteq \mathfrak{D}(m)$. Hence $L(\pi^{m-1}; \pi^m) = J(\pi^{m-1}; \pi^m)$. This is impossible since $\pi^{m-1} \notin L^2 \bmod \pi^m$.

(ii) Suppose if possible that $\chi(L) \neq 0$ for all χ with $m(\chi) = m$. First take $m \leqq e$. Define

$$J \cong \begin{pmatrix} \epsilon\pi^u + \pi^{m-1} & 1 \\ 1 & 0 \end{pmatrix}, \qquad H \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

In virtue of the relation $L \oplus L \doteqdot L \oplus H$ we have $\chi(L) = \chi(H)$. Since $\chi(L) \neq 0$ for all χ with maximal support $\mathfrak{o}(m)$, it follows that $\chi(\delta \circ L) \neq 0$ for any unit δ. In particular, $\chi(J) \neq 0$ when $m(\chi) = m$. Hence $\chi(J) = \chi(H) = \chi(L)$ when $m(\chi) = m$. For the remaining $\chi \in \mathfrak{D}(m)$, $\chi(J) = \chi(L)$ since $J \cong L \bmod \pi^{m-1}$. Hence $L(\epsilon\pi^u; \pi^m) = J(\epsilon\pi^u; \pi^m)$. This is impossible since $\epsilon\pi^u \notin J^2 \bmod \pi^m$.

Now let $m = e + k$ with $k > 0$. Let K be defined by (29). Using the relations $|2\pi^k| = |\pi^m| > |4\pi^{-u}|$ we see that $|\pi^{u+k}| > |2| > |4\pi^{-(u+k)}|$ and so there is a character χ with $m(\chi) = m$ such that $\chi_{(k)}(K) = 0$. Hence $\chi(L) = 0$ by (30).

(iii) Now let $u + m$ be odd. First suppose that $m \leqq e$. Then

$$\begin{aligned}\chi(L) &= \Sigma\Sigma\, \chi(\epsilon\pi^u\alpha^2)\chi(2\alpha\beta)\\ &= 2^{fm}\, \Sigma\, \chi(\epsilon\pi^u\alpha^2)\\ &= 2^{fm}\, \Sigma\Sigma\Sigma\, \chi(\epsilon\pi^u(a + \pi^{\frac{1}{2}(m-1-u)}b + \pi^{\frac{1}{2}(m+1-u)}c)^2)\\ &= 2^{fm}\, \Sigma\, \chi(\epsilon\pi^u a^2)\, \Sigma\, \chi(\epsilon\pi^{m-1}b^2)\, \Sigma\, \chi(\epsilon\pi^{m+1}c^2)\end{aligned}$$

with

$$\alpha \bmod \mathfrak{o}(m),\ \beta \bmod \mathfrak{o}(m),\ a \bmod \mathfrak{o}(\tfrac{1}{2}(m - 1 - u)),\ b \bmod \pi,$$
$$c \bmod \mathfrak{o}(\tfrac{1}{2}(m - 1 + u)).$$

But $\chi_{(m-1)}$ has maximal support $\pi\mathfrak{o}$ and so

$$\Sigma\, \chi(\epsilon\pi^{m-1}b^2) = \Sigma\, \chi_{(m-1)}(\epsilon b^2) = \Sigma\, \chi_{(m-1)}(b) = 0.$$

Hence $\chi(L) = 0$.

Now let $m = e + k$ with $k > 0$. Let K be defined by (29). Then $|\pi^{u+k}| > |2| > |4\pi^{-(u+k)}|$ and so $\chi_{(k)}(K) = 0$. Hence $\chi(L) = 0$ by (30). q. e. d.

Now we can describe the zeros of (25). Let L be a π^0-unitary lattice with fundamental invariants $[\pi^u]$, v, and let $m \geqq 0$ be a fixed rational integer. Then the zeros of $\chi(L)$ with $m(\chi) = m$ are given by

(31) $m \leqq u \quad \Longrightarrow \quad \chi(L) \neq 0$

(32) $u < m \leqq v$ with $u + m$ even $\quad \Longrightarrow \quad$ ambiguous

(33) $u < m \leqq v$ with $u + m$ odd $\quad \Longrightarrow \quad \chi(L) = 0$

(34) $v < m < 2e - v \quad \Longrightarrow \quad \chi(L) = 0$

(35) $2e - v \leqq m < 2e - u$ with $u + m$ odd $\quad \Longrightarrow \quad \chi(L) = 0$

$$(36)\qquad 2e-v \leqq m < 2e-u \text{ with } u+m \text{ even} \qquad \Longrightarrow \qquad \text{ambiguous}$$

$$(37)\qquad 2e-u \leqq m \qquad \Longrightarrow \qquad \chi(L) \neq 0,$$

where $\chi(L)=0$ and $\chi(L)\neq 0$ both have solutions in the ambiguous case.

We prove these equations by referring to the two lemmas. The zeros of $\chi(L)$ are unaltered by adjoining hyperbolic planes; hence assume that $\dim L \geqq 4$. Neither the zeros nor the fundamental invariants are changed by adjoining any unit represented by L; hence assume $\dim L$ even. Write

$$L \cong \begin{pmatrix} \epsilon\pi^u & 1 \\ 1 & \alpha\pi^v \end{pmatrix} \oplus \begin{pmatrix} \pi^v & 1 \\ 1 & \{4\pi^{-v}\} \end{pmatrix} \oplus \sum \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

As above, we can adjoin $\begin{pmatrix} \epsilon\pi^u & 1 \\ 1 & \alpha\pi^v \end{pmatrix}$ to L and we continue to call the enlarged lattice L. Using a determinantal argument we find

$$L \cong \begin{pmatrix} [\pi^u] & 1 \\ 1 & \{4\pi^{-u}\} \end{pmatrix} \oplus \begin{pmatrix} \pi^v & 1 \\ 1 & \{4\pi^{-v}\} \end{pmatrix} \oplus \sum \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Equations (31)-(37) now follow immediately from the two lemmas.

Remark. In the 2-adic case this description of the Gauss sums agrees with the results quoted by Minkowski on p. 57 of [6]. For a discussion of 1-dimensional Gauss sums over number fields see the work of Hecke, especially pp. 218-249 of [4]; compare the results on p. 244 [4] with Lemma 1 of this paper.

6. Unramified theory. We shall see later that it is easy to characterize lattices over local fields in which 2 is a unit and the fact that the Gauss sums never vanish over these fields is responsible for this. The unramified 2-adic theory is almost as easy. To be sure the Gauss sums can vanish, but the zeros take on a very simple form. Thus we apply (31)-(37) to a π^0-unitary lattice L and we find that

$$(38)\qquad \chi(L)=0 \Longleftrightarrow m(\chi)=1 \text{ and } N(L)=\mathfrak{o}.$$

Now let us establish the invariants.

THEOREM 3. *Let* $\operatorname{ord} 2 = 1$. *If L and K are totally integral lattices of the same type such that* $\chi(L)=\chi(K)$ *for all* $\chi \in \mathfrak{D}(3+s(t))$, *then* $L \cong K$.

Proof. First observe that if L and K have canonical decompositions $L=\sum L_\lambda$, $K=\sum K_\lambda$ in which $L_1 \cong K_1$, then

$$(39)\qquad \chi(L_1{}^{\perp}) = \chi(K_1{}^{\perp}) \qquad \text{for } \chi \in \mathfrak{D}(3+s(t)),$$

where $L = L_1 \oplus L_1^{\perp}$, $K = K_1 \oplus K_1^{\perp}$. For we can take $s(1) = 0$. If $\chi(L_1) \neq 0$, we are through by Proposition 1. If $\chi(L_1) = 0$, then χ has maximal support $2\mathfrak{o}$ by (38). But $N(L_1^{\perp}) = N(K_1^{\perp}) \subseteq 2\mathfrak{o}$. Hence $\chi(L_1^{\perp}) = \chi(K_1^{\perp})$. So (39) holds.

Now proceed to the required result by induction to t. By the cancellation law established in Theorem 5.2 of [7], take $\dim L_1 = \dim K_1$ odd, where $L = \sum L_\lambda$, $K = \sum K_\lambda$ are canonical decompositions of L and K. Assume that $s(1) = 1$. For $t = 1$ we are through by Theorem 2. Take $t > 1$. It suffices to prove that

$$\bar{L} = L_0 \oplus L \cong K_0 \oplus K = \bar{K} \text{ where } L_0 \cong 1 \cong K_0,$$

again by Theorem 5.2 of [7]. Note that $\chi(\bar{L}) = \chi(\bar{K})$ for all $\chi \in \mathfrak{D}(3 + s(t))$. Using the decompositions (12)-(14) of [8] on the second components of $\bar{L}$ and $\bar{K}$, it is easy to see that

$$L_0 \oplus L_1 \cong [1] \oplus [2] \oplus \sum \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}.$$

And similarly with $K_0 \oplus K_1$. Cancelling all superfluous π^1-hyperbolic planes, this allows us to assume that $\bar{L}$ and $\bar{K}$ have 1-dimensional π^1-components. Since $\bar{L}$ and $\bar{K}$ represent the same units modulo 8, we can write

$$\bar{L} = L_0' \oplus L', \qquad \bar{K} = K_0' \oplus K', \qquad L_0' \cong K_0' \cong [1].$$

Then by (39) we have $\chi(L') = \chi(K')$ when $\chi \in \mathfrak{D}(3 + s(t))$. Again we get

$$L' = L_1'' \oplus L'', \qquad K' = K_1'' \oplus K'', \qquad L_1'' \cong K_1'' \cong [2],$$

with $\chi(L'') = \chi(K'')$ when $\chi \in \mathfrak{D}(3 + s(t))$. But L'' and K'' are of the same type. Hence by the inductive assumption $L'' \cong K''$. Hence $\bar{L} \cong \bar{K}$. q. e. d.

7. Characterization by Gauss sums. Let us consider two totally integral lattices L and K; suppose that these lattices are of the same type and that their Gauss sums are equal for all characters in $\mathfrak{D}(2e + s(t) + 1)$. If L and K are unitary this implies that $L \cong K$, and so their Gauss sums are equal for all $\chi \in \mathfrak{D}$. In general, the equivalence class of L cannot be determined by Gauss sums alone, but we shall show that all subsequent Gauss sums can be expressed in terms of the Gauss sums modulo $4\pi^{s(t)+1}$. Thus nothing is gained by considering those $\chi \notin \mathfrak{D}(2e + s(t) + 1)$. Before proving this we shall need some preliminary results.

Consider a character with $m(\chi) \geqq 2e+2$. Contention:

$$\sum_{\alpha \bmod \mathfrak{o}(m)} \chi(\alpha^2) = 2^f \sum_{\alpha \bmod \mathfrak{o}(m-2)} \chi_{(2)}(\alpha^2). \tag{40}$$

In virtue of Proposition 2 it suffices to prove

$$2^f \sum_{\alpha \bmod \mathfrak{o}(m)} \chi(\alpha^2) = \sum_{\alpha \bmod \mathfrak{o}(m)} \chi(\pi^2\alpha^2), \tag{41}$$

and this amounts to proving

$$\chi(K)/\chi(L) = 2^f \tag{42}$$

where $L \cong (-1) \oplus (1)$ and $K \cong (-1) \oplus (\pi^2)$. Now

$$L \cong \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}, \qquad K \cong \begin{pmatrix} -1 & \pi \\ \pi & 0 \end{pmatrix}.$$

As in (26)-(28) this leads to $\chi(L) = 2^{mf+ef}$. Similarly we can prove that $\chi(K) = 2^{mf+ef+f}$. Hence (42) holds and the contention is proved.

Proposition 4. *L is a totally integral lattice; χ has maximal support $\mathfrak{o}(m) \subseteq 4\mathfrak{o}(s(t)+2)$. Then $\chi(L) = 2^{nf}\chi_{(2)}(L)$.*

Proof. Write L in the canonical decomposition $L = L_1 \oplus \cdots \oplus L_t$. Define the t-dimensional lattice $I = \Sigma I_\lambda$ with $I_\lambda \cong \pi^{s(\lambda)}$. Then $\chi(I) = 2^{tf}\chi_{(2)}(I)$ in virtue of (40) and Proposition 2. Since $I \oplus L$ has an orthogonal basis, it again follows that $\chi(I \oplus L) = 2^{(t+n)f}\chi_{(2)}(I \oplus L)$. Since $\chi(I) \neq 0$, we have $\chi(L) = 2^{nf}\chi_{(2)}(L)$. q. e. d.

Corollary 1. *If K has the same type as L and $\chi(L) = \chi(K)$ for all $\chi \in \mathfrak{D}(2e+s(t)+1)$, then $\chi(L) = \chi(K)$ for all $\chi \in \mathfrak{D}$. And $L^2 = K^2$.*

Proof. The first part is an immediate consequence of the proposition. Now take $\alpha \in L^2$. Then $\alpha \in K^2 \bmod 4\pi\alpha$ since $L(\alpha; 4\pi\alpha) = K(\alpha; 4\pi\alpha)$. Hence $\alpha \in K^2$ by Hensel's lemma. q. e. d.

Let us consider two lattices L and K which are of the same type and have the same fundamental invariants a_λ, $v(\lambda)$ for $1 \leqq \lambda \leqq t$. Let J be defined as

$$J \cong \begin{pmatrix} a_1 & \pi^{s(1)} \\ \pi^{s(1)} & \pi^{v(1)} \end{pmatrix}.$$

Then

$$J \oplus L \cong J \oplus K \Longrightarrow L \cong K. \tag{43}$$

This can be verified quite easily by applying both the necessity and sufficiency of Theorem 2 of [8]. The proof is left to the reader.

Consider two lattices $I = I_2 \oplus \cdots \oplus I_t$ and $J = J_2 \oplus \cdots \oplus J_t$ which are of the same type and have the same fundamental invariants a_λ, $v(\lambda)$ for $2 \leqq \lambda \leqq t$; also let $s(2) = 1$. We contend that

$$(44) \qquad 0 \leqq m = m(\chi) < 2e + 2 - v(2) \Longrightarrow \chi(I) = \chi(J).$$

In order to prove this we assume that the given decompositions are big and supersaturated; there is no loss of generality in doing this. Clearly $I_\lambda \cong J_\lambda \bmod \pi^{v(\lambda)}$, and so $I_\lambda \cong J_\lambda \bmod \pi^{v(2)}$ for $2 \leqq \lambda \leqq t$. Hence $\chi(I) = \chi(J)$ when $\mathfrak{o}(m) \supseteqq \mathfrak{o}(v(2))$. Now investigate the remaining m, i. e.

$$(45) \qquad |4/\pi^{v(2)-1}| < |\pi^{m-1}| < |\pi^{v(2)-1}|.$$

Then $\chi(I_2) = 2^{n(2)f}\chi_{(1)}(\pi^{-1} \circ I_2)$ in virtue of (9). But $\pi^{-1} \circ I_2$ has fundamental invariants $[\pi^{u(2)-1}]$, $v(2) - 1$; while $\chi_{(1)}$ has maximal support $\mathfrak{o}(m-1)$; hence by (34) and (45) we have $\chi(I_2) = 0$; hence $\chi(I) = 0$ by Proposition 1. By symmetry, $\chi(J) = 0$. This proves the contention.

We shall also need the following. Let I and J be defined by

$$I \cong \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}, \qquad J \cong \begin{pmatrix} a\pi^2 & \pi \\ \pi & 0 \end{pmatrix}, \qquad a \in \mathfrak{o}.$$

Then

$$(46) \qquad \chi(I) = 0 \Longrightarrow \chi(J) = 0 \text{ if } m(\chi) > e.$$

For let us consider $\alpha \bmod \mathfrak{o}(m-1)$, $\beta \bmod \pi$, $\gamma \bmod \mathfrak{o}(m)$. Then

$$\begin{aligned} \chi(J) &= \Sigma\Sigma\Sigma\, \chi(a\pi^2(\alpha + \pi^{m-1}\beta)^2)\chi(2\pi(\alpha + \pi^{m-1}\beta)\gamma) \\ &= 2^f\, \Sigma\Sigma\, \chi(a\pi^2\alpha^2)\chi(2\pi\alpha\gamma) \\ &= 2^f\, \Sigma\Sigma\Sigma\, \chi(a(\beta + \pi\alpha)^2)\chi(2(\beta + \pi\alpha)\gamma) \end{aligned}$$

in virtue of the relation

$$\chi(a(\beta + \pi\alpha)^2) \sum_{\gamma \bmod \mathfrak{o}(m)} \chi(2(\beta + \pi\alpha)\gamma) = 0 \text{ if } |\beta| = 1,$$

which is an immediate consequence of (2). Hence $\chi(J) = 2^f\chi(I) = 0$.

In particular this proves that if

$$G \cong \begin{pmatrix} a & 1 \\ 1 & \delta\pi^v \end{pmatrix} \text{ with } v = v_G(1),\ |\delta| = 1,$$

then for $m(\chi) \geqq 2e - v$ and $m(\chi) > e$,

$$(47) \qquad \chi(G) = 0 \Longrightarrow \chi(J) = 0.$$

For it can easily be verified, for instance by Theorem 2 of [8], that $G \oplus (-1 \circ G) \cong I \oplus \begin{pmatrix} \pi^v & 1 \\ 1 & 0 \end{pmatrix}$. Hence by (37) and (46) we get $\chi(J) = 0$.

Two definitions. The ideal $\mathfrak{f}_j$, $1 \leqq j \leqq t-1$, is defined as in Section 5 of [8]. The ideal $\mathfrak{g}$ is defined as in equation (2) of [8].

THEOREM 4. *L and K are totally integral lattices of the same type and $L = \sum L_\lambda$, $K = \sum K_\lambda$ are canonical decompositions. Then L and K are isometric if and only if for all appropriate λ,*

$$\text{(i)} \qquad v_L(\lambda) = v(\lambda) = v_K(\lambda), \qquad a_\lambda(L) \cong a_\lambda(K) \bmod \pi^{v(\lambda)},$$

$$\text{(ii)} \qquad d(L_1 \oplus \cdots \oplus L_\lambda)/d(K_1 \oplus \cdots \oplus K_\lambda) \cong 1 \bmod \mathfrak{f}_\lambda,$$

$$\text{(iii)} \qquad \chi(L) = \chi(K) \text{ for all } \chi \in \mathfrak{D}(2e + s(t) + 1).$$

Proof. The necessity follows from Theorem 2 of [8]. We shall now establish the sufficiency.

Take $a_\lambda(L) = a_\lambda = a_\lambda(K)$. We proceed by induction on the length $s(t) - s(1)$ of L. We can assume that $s(1) = 0$. The induction can be made to start since the theorem has already been proved for lattices of zero length in Theorem 2. By adjoining suitable hyperbolic planes to L and K, we can suppose that L and K are big. If a_1 is a unit, the enlarged lattices $(a_1) \oplus L$ and $(a_1) \oplus K$ satisfy the conditions of the theorem and it suffices to prove the isometry of the enlarged lattices in virtue of Corollary 3 of [8]. In other words we can assume that L_1 and K_1 are of even dimension.

Suppose that $u(1) = e$. If $u(2) = e$, we can find new decompositions $L = \sum L_\lambda$, $K = \sum K_\lambda$ in which L_1 and K_1 are orthogonal sums of hyperbolic planes. The complements of L_1, K_1 in L, K then satisfy the conditions of the theorem and so we are through. If $u(2) \geqq e + 1$, then $\mathfrak{f}_1 \subseteq 4\pi\mathfrak{o}$, hence $d(L_1) \cong d(K_1)$ in the original decompositions, hence $L_1 \cong K_1$. Induction again gets us through. We shall therefore assume that $u(1) < e$.

The next step in the reduction of the problem is to show that we can take $s(2) = 1$. Suppose $s(2) > 1$. Define N_* as the 12-dimensional lattice consisting of the orthogonal sum of six π^1-hyperbolic planes. Define L^* and K^* by the canonical decompositions

$$L^* = L_1 \oplus N_* \oplus L_2 \oplus \cdots \oplus L_t, \qquad K^* = K_1 \oplus N_* \oplus K_2 \oplus \cdots \oplus K_t.$$

It suffices to prove that $L^* \cong K^*$. To this end we show that L^* and K^* which are still of length $s(t) - s(1)$ also satisfy (i)-(iii). It follows immediately from their definition that a_λ and $v(\lambda)$ have the same values for L^*, K^* as for L, K when $\lambda = 1, 2, \cdots, t$. If a_* and $v(*)$ describe $L_{(1)}{}^*$ they also describe $K_{(1)}{}^*$. We know that

$$| a_1 \pi^2 | \leqq | a_* | \leqq | a_1 |.$$

It is now clear that (i) and (iii) hold for L^*, K^*. (ii) is true when $\lambda = 2, 3, \cdots, t-1$. Let us write $\mathfrak{f}_1{}^*, \mathfrak{f}_*, \mathfrak{f}_2, \cdots, \mathfrak{f}_{t-1}$ for the $\mathfrak{f}$'s of L^*, K^*. Then it is enough to prove

$$\mathfrak{f}_1{}^* \supseteq \mathfrak{f}_1, \qquad \mathfrak{f}_* \supseteq \mathfrak{f}_1. \tag{48}$$

First consider $u(2) = u(1)$ or $u(2) = u(1) + 1$. Using (23)-(24) of [8] it is easily seen that

$$\mathfrak{f}_1 = \pi^{u(1)+v(1)}\mathfrak{o}, \qquad \mathfrak{f}_1{}^* = \pi^{u(1)+v(1)}\mathfrak{o}, \qquad \pi^2\mathfrak{f}_* = \pi^{u(2)+v(*)}\mathfrak{o}.$$

If $u(2) = u(1)$ we get (48) from the inequality $v(*) \leqq v(1) + 2$; if $u(2) = u(1) + 1$ we get (48) from $v(*) = u(1) + 2$, $u(2) = v(1)$. Now consider $u(2) \geqq u(1) + 2$; then $u(*) = u(1) + 2$, $v(*) \leqq v(1) + 2$, and $\mathfrak{f}_1{}^* = \pi^{u(1)+v(*)}\mathfrak{o}$. But

$$\mathfrak{f}_1 = [\pi^{u(1)+u(2)}\mathfrak{g}(a_1a_2),\ \pi^{u(1)+v(2)},\ \pi^{u(2)+v(1)},\ 2\pi^{\frac{1}{2}(u(1)+u(2))}]$$

$$\pi^2\mathfrak{f}_* = [\pi^{u(*)+u(2)}\mathfrak{g}(a_1a_2),\ \pi^{u(*)+v(2)},\ \pi^{u(2)+v(*)},\ 2\pi^{\frac{1}{2}(u(*)+u(2))+1}].$$

the quantities $2\pi^{\frac{1}{2}(u(1)+u(2))}$, $2\pi^{\frac{1}{2}(u(*)+u(2))+1}$ appearing only when $u(1) + u(2)$ is even. So clearly $\mathfrak{f}_* \supseteq \mathfrak{f}_1$; and $\mathfrak{f}_1{}^* \supseteq \mathfrak{f}_1$ since $|\pi^{u(2)}\mathfrak{g}(a_1a_2)| \leqq |\pi^{v(*)}|$. Thus (48) is generally true. We accordingly assume that the *given* L and K have $s(2) = 1$.

If the decompositions ΣL_λ, ΣK_λ of the given L, K are varied, conditions (i)-(iii) remain valid. Only (ii) needs to be verified and this follows from the necessity of the theorem. In particular, we can assume that ΣL_λ and ΣK_λ are supersaturated.

A final step in the reduction. Call a canonical decomposition $J = \Sigma J_\lambda$ *simple* if all J_λ are big and supersaturated, $2 \leqq \lambda \leqq t$, while J_1 represents $[\pi^{u(1)}]$, $[\pi^{v(1)}]$, and

$$J_1 \cong \begin{pmatrix} [\pi^{u(1)}] & 1 \\ 1 & \{\pi^{u(1)}\} \end{pmatrix} \oplus \Sigma \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \tag{49}$$

we do not insist that J_1 be big; note that

$$J_1 \cong \begin{pmatrix} [\pi^{u(1)}] & 1 \\ 1 & [\pi^{v(1)}] \end{pmatrix} \oplus \Sigma \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ if } v(1) < e. \tag{50}$$

We shall show that ΣL_λ, ΣK_λ can always be assumed simple. If $u(2) = u(1)$ or $u(2) = u(1) + 1$, using the "op" transformations in conjunction with Proposition 6 of [8], we can find simple decompositions for L and K. Now consider $u(2) = u(1) + 2$. If $v(2) = v(1)$ we proceed as above to simple decompositions for L and K. So let $v(2) > v(1)$. Then $|\mathfrak{f}_1| < |\pi^{u(1)+v(1)}|$. So one of two things can happen. Either

$$(51)\quad d(L_1) \cong (-1)^{\frac{1}{2}n(1)}(1+[\pi^{u(1)+v(1)}]),\qquad d(K_1) \cong (-1)^{\frac{1}{2}n(1)}(1+[\pi^{u(1)+v(1)}]),$$

or

$$(52)\quad d(L_1) \cong (-1)^{\frac{1}{2}n(1)}(1+\{\pi^{u(1)+v(1)+1}\}),\qquad d(K_1) \cong (-1)^{\frac{1}{2}n(1)}(1+\{\pi^{u(1)+v(1)+1}\}),$$

where $\dim L_1 = \dim K_1 = n(1)$. In the first case $\sum L_\lambda$, $\sum K_\lambda$ are simple by (12). In the second case adjoin $\begin{pmatrix} a_1 & 1 \\ 1 & \pi^{v(1)} \end{pmatrix}$ to both L and K, and we see that the corresponding decompositions of the enlarged lattices satisfy (51) and are therefore simple. Moreover, the enlarged lattices satisfy the conditions of the theorem since their fundamental invariants are unchanged by the adjunction; and it suffices to prove the isometry of the enlarged lattices in virtue of (43). In general therefore, we can assume that $\sum L_\lambda$, $\sum K_\lambda$ are simple. Cancelling off hyperbolic planes allows us to take $\dim L_1 = \dim K_1 = 2$.

So much for the reduction of the problem. To sum up, assume that the sufficiency holds for lattices of length less than $s(t) - s(1)$, and establish it for the simple decompositions $L = \sum L_\lambda$, $K = \sum K_\lambda$ which satisfy the conditions of the theorem and are such that

$$(53)\qquad u(1) < e,\quad s(1) = 0,\quad s(2) = 1,\quad \dim L_1 = \dim K_1 = 2.$$

Case 1. $u(2) = u(1)$. By means of the "op" transformations we can write

$$L = L_1' \oplus L_2' \oplus L_3 \oplus \cdots \oplus L_t,\qquad K = K_1' \oplus K_2' \oplus K_3 \oplus \cdots \oplus K_t$$

with L_2', K_2' supersaturated and

$$(54)\qquad L_1' \cong \begin{pmatrix} \pi^{v(1)} & 1 \\ 1 & 4\alpha\pi^{-v(1)} \end{pmatrix},\qquad K_1' \cong \begin{pmatrix} \pi^{v(1)} & 1 \\ 1 & 4\beta\pi^{-v(1)} \end{pmatrix}.$$

Put $L' = L_2' \oplus L_3 \oplus \cdots \oplus L_t$ and similarly define K'. If $u(1)+v(1)$ is even, then $v(1) = e$ and we can assume that $\alpha = \beta = 0$ in (54). Then L', K' satisfy (i)-(iii) and so $L' \cong K'$. From now on take $u(1)+v(1)$ odd. If $v(1) < e$, then $|\pi^{v(2)}| \geqq |\pi^{v(1)+2}| \geqq |4\pi^{-v(1)}|$, and we can again assume that $\alpha = \beta = 0$. Then (i)-(ii) are immediate for L', K'. We must show that $\chi(L') = \chi(K')$, for all $\chi \in \mathfrak{D}(2e + s(t) + 1)$. By (44) we can assume that $m(\chi) \geqq 2e + 2 - v(2)$; then $m(\chi) \geqq 2e - v(1)$ and so $\chi(L_1') \neq 0$; thus $\chi(L') = \chi(K')$ by division, in virtue of Proposition 1. Hence $L' \cong K'$ by the inductive assumption.

To conclude this case we must consider $u(1)+v(1)$ odd, $v(1) = e$.

If $v(1)=v(2)=e$ the result is trivial since we can take $\alpha=\beta=0$. So let $v(2)=v(1)+1=e+1$. If $(1+4\alpha)\cong(1+4\beta)$ we are through. So suppose that $(1+4\alpha)/(1+4\beta)$ is a non-square. We shall prove this impossible. Define $I\cong 1\cong J$. Then $I\oplus(\pi^e\circ L)$ and $J\oplus(\pi^e\circ K)$ have the same Gauss sums modulo 4π. But

$$I\oplus(\pi^e\circ L)\cong(1+4\alpha)\oplus\begin{pmatrix}0&2\\2&0\end{pmatrix}\oplus(\pi^e\circ L').$$

And similarly with K. Hence $(1+4\alpha)\oplus(\pi^e\circ L')$ represents $1+4\beta$. But $(\pi^e\circ L')$ represents no number of even ordinal $\geqq 2e$. So $(1+4\alpha)\oplus(\pi^e\circ L')$ cannot represent $1+4\beta$. This is a contradiction. Thus the first case is proved.

Case 2. $u(2)=u(1)+1$. We have $u(1)<e$; thus $v(2)=u(1)+2$. Using the "op" transformations and Proposition 6 of [8] we can write

$$L=L_1'\oplus L_2'\oplus L_3\oplus\cdots\oplus L_t,\qquad K=K_1'\oplus K_2'\oplus K_3\oplus\cdots\oplus K_t,$$

where L_2', K_2' are supersaturated and

$$L_1'\cong\begin{pmatrix}\pi^{u(1)}&1\\1&0\end{pmatrix},\qquad K_1'\cong\begin{pmatrix}\pi^{u(1)}&1\\1&0\end{pmatrix}.$$

Let L', K' denote the complements of L_1', K_1' in L, K respectively. Clearly L', K' continue to satisfy (i)-(ii); we must establish (iii). In virtue of (44) we need only consider $m(\chi)\geqq 2e-u(1)$; thus $\chi(L_1')\neq 0$; thus $\chi(L')=\chi(K')$ by division. By the inductive assumption we again get $L'\cong K'$. This proves the second case.

Case 3. $u(2)=u(1)+2$. We can assume that $a_1\in L^2$; then $a_1\in K^2$ by Corollary 1. We can assume that $u(1)<e$, $a_2=a_1\pi^2$, $v(2)\geqq v(1)\geqq v(2)-2$. Since ΣL_λ and ΣK_λ are simple we have

$$(55)\qquad d(L_1)\cong-(1+[\pi^{u(1)+v(1)}]),\qquad d(K_1)\cong-(1+[\pi^{u(1)+v(1)}])$$

when $u(1)+v(1)$ is odd. Now L represents a_1, and L_2 represents all numbers represented by $L_2\oplus\cdots\oplus L_t$. So it is easily seen that we can write

$$L_1\oplus L_2=\bar{L}_1\oplus\bar{L}_2\text{ with }\bar{L}_1\cong\begin{pmatrix}a_1&1\\1&\{\pi^{v(1)}\}\end{pmatrix}$$

where $\bar{L}_2$ is still a supersaturated component. Similarly define $\bar{K}_1\oplus\bar{K}_2$

$= K_1 \oplus K_2$. If $v(1) = v(2)$ or if $u(1) + v(1)$ is even, we easily see that we can take

$$\bar{L}_1 \cong \begin{pmatrix} a_1 & 1 \\ 1 & [\pi^{v(1)}] \end{pmatrix}, \quad \bar{K}_1 \cong \begin{pmatrix} a_1 & 1 \\ 1 & [\pi^{v(1)}] \end{pmatrix}. \tag{56}$$

While if $v(2) > v(1)$ with $u(1) + v(1)$ odd, we have $|\mathfrak{f}_1| < |\pi^{u(1)+v(1)}|$, thus $\bar{L}_1$, $\bar{K}_1$ satisfy (55), thus (56) is true for suitably chosen $\bar{L}_1$, $\bar{K}_1$. Write

$$\bar{L}_1 \cong \begin{pmatrix} a_1 & 1 \\ 1 & \delta\pi^{v(1)} \end{pmatrix} \text{ with } |\delta| = 1. \tag{57}$$

Since $d(\bar{L}_1) \cong d(\bar{K}_1) \bmod \pi^{u(1)+v(2)}$, using Theorem 14.3 of [7] we can write

$$\bar{K}_1 \cong \begin{pmatrix} a_1 & 1 \\ 1 & \delta\pi^{v(1)} + \{\pi^{v(2)}\} \end{pmatrix}.$$

Using Proposition 6 of [8], we can find a decomposition $K_1' \oplus K_2' = \bar{K}_1 \oplus \bar{K}_2$ in which K_2' is still supersaturated, and $K_1' \cong \bar{L}_1'$. In other words, we have two simple decompositions $L = \Sigma L_\chi'$, $K = \Sigma K_\chi'$ in which $L_1' \cong K_1'$ have the form of (57). If L', K' are the complements of L_1', K_1' in L, K respectively, we must show that L', K' satisfy the conditions of the theorem. Once this is verified the isometry $L \cong K$ follows by the inductive assumption. (i) and (ii) are easily checked for L', K'; we must establish (iii) for these lattices.

If $m(\chi) < 2e + 2 - v(2)$, we have $\chi(L') = \chi(K')$ by (44). Now let $m(\chi) \geqq 2e + 2 - v(2)$. Then $m(\chi) \geqq 2e - v(1)$ and $m(\chi) > e$, since $2 + v(1) \geqq v(2)$ and $v(2) \leqq e + 1$. If $\chi(L_1') = \chi(K_1') = 0$, we see that L_2' and K_2' each have a component of the form

$$\begin{pmatrix} a_1\pi^2 & \pi \\ \pi & 0 \end{pmatrix}$$

and so $\chi(L') = 0 = \chi(K')$ in virtue of (47). While if $\chi(L_1') = \chi(K_1') \neq 0$, then $\chi(L') = \chi(K')$ by division. Hence L' and K' have the same Gauss sums. This proves the theorem.

In general it is impossible to determine the integral equivalence of lattices by Gauss sums alone, and this point will be illustrated in the next section. All that can be said about lattices with the same Gauss sums is that they are fractionally equivalent; obviously the converse does not hold.

THEOREM 5. *L and K are totally integral lattices of the same type and $\chi(L) = \chi(K)$ for all $\chi \in \mathfrak{D}(2e + s(t) + 1)$. Then L and K are fractionally equivalent.*

Proof. In virtue of Witt's cancellation theorem [11] we can adjoin as many 1-dimensional lattices to L and K as we please. So assume that we have canonical decompositions $L = \sum L_\lambda$, $K = \sum K_\lambda$ in which each component is proper with $s(\lambda+1) = s(\lambda) + 1$. The fundamental invariants can then be chosen as

$$a_\lambda = \pi^{s(\lambda)}, \qquad v(\lambda) = s(\lambda) + 1, \qquad \mathfrak{f}_\lambda = \pi\mathfrak{o},$$

for both L and K. Hence $L \cong K$ by Theorem 4. q. e. d.

8. Remarks. By way of example we shall make some rough estimates of the Gauss sums. χ will be a fixed character with maximal support $\mathfrak{o}(m)$. We put

$$h = 2^{2mf} \text{ if } m \leqq e, \qquad h = 2^{mf+ef} \text{ if } m \geqq e.$$

Refining the method used to derive (15) it is easy to see that $\chi(H) = h$ for the unit hyperbolic plane H. Now consider the π^0-unitary lattices

$$J_0 \cong \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}, \qquad J \cong \begin{pmatrix} a & 1 \\ 1 & b \end{pmatrix}.$$

Then $\chi(J_0) = h$ whenever $\chi(J_0) \neq 0$, since $J_0 \otimes J_0 \cong J_0 \otimes H$. Using this result in conjunction with the isometry

$$J \oplus J \oplus J \oplus J \cong \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} \beta & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} \beta & 1 \\ 1 & 0 \end{pmatrix},$$

we get $\chi(J) = \omega_4 h$ whenever $\chi(J) \neq 0$, where ω_4 denotes some complex 4-th root of unity. So if I is a 1-dimensional π^0-unitary lattice, we have $\chi(I) = \omega_8 h^{\frac{1}{2}}$, where ω_8 is an 8-th root of unity. Thus for the n-dimensional π^0-unitary lattice L we have

$$\chi(L) = 0 \text{ or } \chi(L) = \omega h^{\frac{1}{2}n} \tag{58}$$

where ω is one of the complex 8-th roots of unity.

Now three examples to show the part played by the various assumptions in Theorems 3 and 4. First consider the 2-adic forms

$$L \cong 1 \oplus 2 \oplus 2 \oplus -2 \oplus 4, \qquad K \cong 1 \oplus 1 \oplus 2 \oplus -4 \oplus 4.$$

Clearly these two forms are not of the same type. Nevertheless they have the same Gauss sums. To see this consider the character χ with maximal support $\mathfrak{p} \subseteq \pi\mathfrak{o}$. For $\mathfrak{p} \supseteq 8\mathfrak{o}$ we have $\chi(L) = \chi(K) = 0$. For $\mathfrak{p} \supseteq 16\mathfrak{o}$ it is easily verified that the two lattices

$$2 \oplus -2 \cong \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix} \quad \text{and} \quad 1 \oplus -4 \cong \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}$$

have the same Gauss sums when computed for the given χ. So the assertion is proved.

Now consider any ramified extension of the 2-adic numbers, with ramification index $e \geqq 6$. Define

$$I \cong \begin{pmatrix} \pi & 1 \\ 1 & 0 \end{pmatrix} \oplus (1), \qquad \cong \begin{pmatrix} \pi & 1 \\ 1 & 0 \end{pmatrix} \oplus (1+\pi), \qquad K \cong \begin{pmatrix} \pi^3 & 1 \\ 1 & 0 \end{pmatrix} \oplus (1).$$

Then the lattices

$$M = I \oplus (\pi^2 \circ J) \quad \text{and} \quad N = J \oplus (\pi^2 \circ I)$$

do not satisfy condition (ii) of Theorem 4. We prove that their Gauss sums are equal. For $\mathfrak{p} \supseteq 4\pi\mathfrak{o}$ we have $\chi(M) = \chi(N) = 0$. For $\mathfrak{p} \subseteq 4\pi^2\mathfrak{o}$ we have $\chi(M) = \chi(N)$ in virtue of the isometry

$$(1) \oplus (-\pi) \oplus \pi^2(1+\pi) \cong (1+\pi) \oplus (-\pi) \oplus (\pi^2).$$

There is another example which shows that the equality of the Gauss sums does not necessarily imply the equality of the fundamental invariants. Consider

$$P = I \oplus (\pi^2 \circ I) \oplus (\pi^4 \circ I), \qquad Q = I \oplus (\pi^2 \circ K) \oplus (\pi^4 \circ I).$$

Then $v_P(2) \neq v_Q(2)$. But $\chi(P) = \chi(Q) = 0$ when $\mathfrak{p} \supseteq 4\pi^3\mathfrak{o}$. And if $\mathfrak{p} \subseteq 4\pi^4\mathfrak{o}$ we have $\chi(P) = \chi(Q)$ in virtue of the relation

$$\begin{pmatrix} \pi^3 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} -\pi & 1 \\ 1 & 0 \end{pmatrix} \cong \begin{pmatrix} \pi & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} -\pi & 1 \\ 1 & 0 \end{pmatrix}.$$

9. At the odd primes. The discussion of the theory over fields in which 2 is a unit is almost trivial. Thus, consider a local field F whose residue class field is a finite field containing p^f elements, $p > 2$. Again we can define the character group $\mathfrak{D}$. For any integral lattice, define the Gauss sums $\chi(L;\pi^r)$ and $\chi(L)$ as in Section 2. Propositions 1-3 are obviously valid. If I is a 1-dimensional π^0-unitary lattice, $-I \oplus I$ is a hyperbolic plane H; it is easily seen that $\chi(H) > 0$; hence $\chi(I) \neq 0$.

THEOREM 6. *L and K are n-dimensional integral lattices over a ring $\mathfrak{o}$ in which 2 is a unit. Then $K \cong L$ if and only if $\chi(K) = \chi(L)$ for all $\chi \in \mathfrak{D}(s_L(t) + 1)$.*

Proof. Induction to n. Write $L = I \oplus I^{\perp}$ with $N(L) = N(I)$ and $I \cong a_1$. Then $a_1 \in K^2 \bmod \pi a_1$. Hence $a_1 \in K^2$ by Hensel's lemma. But $N(K) = N(L) = a_1\mathfrak{o}$ since L and K represent the same numbers modulo

$\mathfrak{o}(s_L(t)+1)$. Hence there is a $J \cong I$ such that $K = J \oplus J^{\perp}$. But $\chi(J^{\perp}) = \chi(I^{\perp})$ for all $\chi \in \mathfrak{D}(s_L(t)+1)$, by division. Hence $J^{\perp} \cong I^{\perp}$. Hence $K \cong L$. q. e. d.

PRINCETON UNIVERSITY.

REFERENCES.

[1] E. Artin, *Algebraic numbers and algebraic functions I*, Princeton University and New York University, 1950-1951.

[2] W. H. Durfee, "Congruence of quadratic forms over valuation rings," *Duke Mathematical Journal*, vol. 11 (1944), pp. 687-697.

[3] E. Hecke, "Reziprozitätsgesetz und Gauss'sche Summen in quadratischen Zahlkörpern," *Gött. Nachr., Math.-phys. Kl.*, pp. 265-278, 1919.

[4] ———, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig, 1923.

[5] B. W. Jones, "A canonical quadratic form for the ring of 2-adic integers," *Duke Mathematical Journal*, vol. 11 (1944), pp. 715-727.

[6] H. Minkowski, "Théorie des formes quadratiques," *Gesammelte Abhandlungen*, Leipzig and Berlin, 1911.

[7] O. T. O'Meara, "Quadratic forms over local fields," *American Journal of Mathematics*, vol. 77 (1955), pp. 87-116.

[8] ———, "Integral equivalence of quadratic forms in ramified local fields," *American Journal of Mathematics*, vol. 79 (1957), pp. 157-186.

[9] G. Pall, "The arithmetical invariants of quadratic forms," *Bulletin of the American Mathematical Society*, vol. 51 (1945), pp. 185-197.

[10] B. L. van der Waerden, *Modern Algebra*, vol. 2, New York, 1950.

[11] E. Witt, "Theorie der quadratischen Formen in beliebigen Körpern," *Journal für die reine und angewandte Mathematik*, vol. 176 (1937), pp. 31-44.

ON THE EXISTENCE OF AN ABSOLUTE CONSTANT CONCERNING "FLAT" OSCILLATORS.*

By AUREL WINTNER.

For large positive t, let $\omega(t)$ be a positive continuous function corresponding to which the differential equation $(*)$ $x'' + \omega^2(t)x = 0$ has the following property: $x'(t) \to 0$, as $t \to \infty$, holds for the derivative of every solution $x(t)$ of $(*)$. Then $(*)$ will be called *flat* (all of its solutions "flatten out"; still, they can be "wobbly" and "large," as shown by the example $\omega(t) = c/t$, mentioned below for $c > \frac{1}{2}$).

Since $x(t) = o(t)$ is necessary for $x'(t) = o(1)$, the "frequency" $\omega(t) > 0$ cannot be "too small" (for large t) if $(*)$ is flat. In fact, $(*)$ will have solutions satisfying $x(t) \sim t$ if the integral of $t\omega^2(t)$ over const. $\leqq t < \infty$ is finite (Bôcher); for instance, if $\omega(t) = O(t^{-1-\epsilon})$ for some $\epsilon > 0$. Crucial proves to be the limiting case $\epsilon = 0$, since the issue then involves the numerical value of the constant absorbed by the O of the assumption $\omega(t) = O(t^{-1})$. Put therefore $[\omega] = \limsup t\omega(t)$, and assume that $[\omega] < \infty$.†

Let α be the greatest universal constant having the property that $(*)$ is non-oscillatory whenever $[\omega] < \alpha$, and let β be the greatest universal constant (if any) having the property that $(*)$ is flat whenever $[\omega] < \beta$. It is well-known that $\alpha = \frac{1}{2}$ (cf., e.g., pp. 231-233 Bieberbach's *Differentialgleichungen* of 1956). If $\omega(t) = c/t$, where $c > \frac{1}{2}$, then the solutions $x(t)$ of $(*)$ are superpositions of the real and imaginary parts of $t^{\frac{1}{2}}\exp(iC\log t)$, where $C = C(c)$ is positive (and tends to 0 as $c \to \infty$, and to ∞ as $c \to \frac{1}{2} + 0$; if $c = \frac{1}{2}$, these solutions $x(t)$ degenerate into $t^{\frac{1}{2}}$ and $t^{\frac{1}{2}}\log t$, so that $(*)$ ceases to be oscillatory).

For this explicity integrable "slow oscillator," $x'(t)$ is $O(t^{-\frac{1}{2}}) = o(1)$, hence (*) is flat; and every $[\omega] > \frac{1}{2}$ is allowed, since $[\omega] = c$, where $\frac{1}{2} < c < \infty$. Thus, in view of the definitions of α and β, one might expect that either $\beta = \alpha$ or $\beta = \infty$. But a theorem of Boas, Boas and Levinson (Duke Math. Journ., vol. 8 (1942), p. 849) implies that (*) is flat whenever $[\omega] < 1$ (provided that (*) is oscillatory; otherwise they conclude from $[\omega] < 1$ the existence of a finite limit $x'(\infty)$, which need not be 0). Hence $\beta \geqq 1$, while $\alpha = \frac{1}{2}$, and so $\beta \neq \alpha$. Consequently, the expected alternative reduces to $\beta = \infty$.

---

* Received February 26, 1957.

† If $[\omega] < \infty$, then $x''(t) = o(t^{-2})x(t)$, by $(*)$, hence $x''(t) = o(t^{-1})$ if $x(t) = o(t)$. It follows therefore from a well-known inequality (which goes back to Hadamard; cf. p. 12 of Carleman's *Fonctions quasi analytiques*, Paris, 1926) that if $[\omega] < \infty$, then $x'(t) = o(1)$ whenever $x(t) = o(t)$. Accordingly, if $[\omega] < \infty$, then $(*)$ is flat *if and only if* $x(t) = o(t)$ holds for all solutions of $(*)$.

It turns out, however, that $\beta = \infty$ is false; in other words, that *an oscillator* (*) *need not be flat if* $\omega(t) = O(t^{-1})$. In order to shorten the formulae, only $\beta < \infty$ will be proved; but the approach to be followed (patterned after my note in the Journ. of Appl. Physics, vol. 18 (1947), pp. 941-942, where a question in "high frequency" $\omega(t)$, rather than the finer question of the present "low frequency" $\omega(t)$, is considered) is flexible enough to lead to $\beta < 1 + \epsilon$ for every $\epsilon > 0$ and therefore, since $\beta \geqq 1$, to $\beta = 1$.

Try to satisfy (*) by $x(t) = r\cos(C\log t)$, where $C = \text{const.} > 0$, $1 \leqq t < \infty$ and $r = r(t)$. Direct substitution leads to the following determination of $\omega(t)$ in terms of $r(t)$:

$$\omega^2 = -r''/r + \{2t^{-1}Cr'/r - Ct^{-2}\}\tan + C^2/t^2, \tag{1}$$

where the argument of tan (and, subsequently, of cos and sin) is $C\log t$, that of the cos in $x(t)$. In order to keep $\omega^2(t)$ continuous, the coefficient { } of tan must be so chosen as to cancel the poles of tan.

Such a choice is $\{\ \} = \phi\cos$, if $\phi = \phi(t)$ is continuous. Choose $\phi(t) = 6t^{-2}\cos$. Then (1) reduces to

$$t^2\omega^2(t) = -t^2r''/r + 6\sin\cos + C^2, \tag{2}$$

and $r = r(t)$ follows from $\{\ \} = 6t^{-2}\cos^2$ by a quadrature:

$$r(t) = \exp\int^t \tfrac{1}{2}s^{-1}(1 + 6C^{-1}\cos^2(C\log s))\,ds. \tag{3}$$

Since the substitution $u = C\log s$ shows that $\int^t s^{-1}\cos^2(C\log s)\,ds \sim \frac{1}{2}C\log t$ as $t \to \infty$, it is seen from (3) that $\log r(t) \sim 2\log t$, hence $r(t) \neq o(t)$. It follows therefore from $x(t) = r(t)\cos$ that $x(t) \neq o(t)$. Hence $x'(t) \neq o(1)$, which means that (*) cannot be flat.

On the other hand, two differentiations of (3) show that

$$t^2r''/r = (\tfrac{1}{2} + 3C^{-1}\cos^2)^2 - (\tfrac{1}{2} + 3C^{-1}\cos^2) - 6\sin\cos. \tag{4}$$

But the function (4) stays bounded, uniformly in t, as $C \to \infty$. It follows therefore from (2) and (4) that, if the value of the constant C is chosen large enough, the resulting coefficient of (*) will satisfy both requirements $\omega^2(t) > 0$, $\omega(t) = O(t^{-1})$.

* *
*

About the only thing for what $\omega^2(t) = O(t^{-2})$ alone (without a restriction of the value of $[\omega]$) will suffice is an estimate of the consecutive zeros, say $t_0, t_1, \cdots, t_n, \cdots$, of a solution $x(t) \not\equiv 0$ of (*), provided that (*) is oscillatory at all (that is, that the sequence $t_0, t_1, \cdots$ is infinite). In fact, $[\omega] < \infty$ alone insures that, as $n \to \infty$,

$$(5) \qquad t_{n+1} - t_n > (1+\gamma)^n, \text{ where } \gamma = \text{const.} > 0,$$

provided that (*) is oscillatory.

Actually, (5) *holds whenever*

$$(6) \qquad \int_t^\infty \omega^2(s)\,ds = O(t^{-1}),$$

where the convergence of $\int^\infty \omega^2(t)\,dt$ is part of the assumption. Needless to say, (6) is a relaxed form of $[\omega] < \infty$ of $\omega(t) = O(t^{-1})$.

First, if a solution $x(t) \not\equiv 0$ of (*) vanishes at both end-points of a t-interval (a, b), then, according to Liapounoff, the integral or $\omega^2(t)$ over (a, b) must exceed the value of $4/(b-a)$ (for a simple proof, cf. pp. 52-53 of Geronimus' *A. M. Ljapunow,* Berlin, 1954). If this is applied to $(a, b) = (t_n, t_{n+1})$, it follows from (6) that $(t_{n+1} - t_n)^{-1} = O(t_n^{-1})$ as $n \to \infty$. But this is equivalent to $\liminf t_{n+1}/t_n > 1$, which proves (5).

THE JOHNS HOPKINS UNIVERSITY.

Proof that these Φ are strip maps. If ϕ is defined on a submanifold U of X and U' denotes the set of all points x of $B(X)$ with $p_X(x) \in U$, then Φ maps $U' \times \Delta(G)$ 1-1 onto $\pi^{-1}(U')$, with Φ and its inverse both C^∞. Also, any two such maps Φ, Φ' differ along a fibre $\pi^{-1}((x, \bar{e}_1, \cdots, \bar{e}_N))$ by a translation $L_{\Delta(g)}$; and, in fact, g depends on x, but is independent of the frame $\bar{e}_1, \cdots, \bar{e}_N$ at x.

$(B, X, O(X) \times \Delta(G), O(X) \times \Delta(G), p_X \circ \pi)$. The following maps $\bar{\Phi}$ make this into a bundle: If ϕ^X is a strip map of $\mathfrak{B}(X)$ and Φ is a strip map of $(B, B(X), \Delta(G), \Delta(G), \pi)$, then $\bar{\Phi}(x, r \times \Delta(g)) = \Phi(\phi^X(x, r), \Delta(g))$, $r \in O(X)$. The $\bar{\Phi}$'s are strip maps, since any two differ along a fibre by a translation of $O(X) \times \Delta(G)$ (this is a consequence of the fact that the element $\Delta(g)$ of the preceding paragraph is independent of the frame at x, i. e., independent of r).

LEMMA 1. *Let $\phi, \phi^X, \phi^X, \phi^M$ be strip maps of the bundles (M, X, F, G, p), $\mathfrak{B}(X), \mathfrak{B}(F), \mathfrak{B}(M)$; let Φ be the strip map of $(B, B(X), \Delta(G), \Delta(G), \pi)$ defined as above in terms of ϕ. Then:*

(1) *given ϕ, ϕ^X on θ^X, and ϕ^F on θ^F, (θ^X, θ^F submanifolds of X, F) there exists a ϕ^M on $\phi(\theta^X, \theta^F)$ such that $\phi^M(\phi(x,f), r \oplus \Delta) = \Phi(\phi^X(x, r), \phi^F(f, \Delta))$ for any $x \in \theta^X$, $f \in \theta^F$, and $r \oplus \Delta \in O(X) \oplus \Delta(K)$;*

(2) *give ϕ^M on some submanifold θ^M of M, there exist ϕ, ϕ^X on some θ^X, and ϕ^F on some θ^F, such that $\phi(\theta^X, \theta^F) \subset \theta^M$ and $\phi^M(\phi(x,f), r \oplus \Delta) = \Phi(\phi^X(x, r), \phi^F(f, \Delta))$ for any $x \in \theta^X$, $f \in \theta^F$, and $r \oplus \Delta \in O(X) \oplus \Delta(K)$.*

Proof. This is a consequence of the definition of Φ in terms of ϕ, and of the type of strip map ϕ^M considered in $\mathfrak{B}(M)$.

Curvature. A choice of coordinates x_i', y_i' in neighborhoods in X, F, and a strip map ϕ of the bundle (M, X, F, G, p), define coordinates on an M-neighborhood. These, together with coordinates s_i', t_i' on $O(X)$ and $\Delta(K)$ and a strip map ϕ^M of $\mathfrak{B}(M)$, define coordinates x_i, y_i, s_i, t_i on a submanifold of B. We denote partial derivatives in the coordinate directions by X_i, Y_i, S_i, T_i. Then a change of coordinates or strip maps (new coordinates being denoted by bars) sends each S_i into a linear combination of the $\bar{S}_j$, each T_i into a linear combination of the $\bar{T}_j$, and each Y_i into a linear combination of the $\bar{Y}_j$ and $\bar{T}_j$ (the Y_j and T_j span the space of vertical vectors of B with respect to the bundle $(B, B(X), \Delta(G), \Delta(G), \pi)$, as do the $\bar{Y}_j$ and $\bar{T}_j$.)

If $\tilde{m}$ is a point of B and $m = p_M(\tilde{m})$, then $S_i(\tilde{m}) = \phi_m{}^M(t \oplus 0)$ for some strip map ϕ^M of $\mathfrak{B}(M)$ and some vector t of $O(X)$. Conversely, every vector of the form $\phi_m{}^M(t \oplus 0)$ is a linear combination of the S_j.

Notation. A point $(m, e_1, \cdots, e_N, f_1, \cdots, f_n)$ will be denoted by (m, e_i, f_i); similarly, points $(x, e_1, \cdots, e_N)$ and $(f, f_1, \cdots, f_n)$ will be denoted by (x, e_i) and (f, f_i).

LEMMA 2. *Let Δg be an element of $\Delta(G)$ and $\tilde{m}$ a point of B. Then $R_{\Delta g} S_i(\tilde{m}) = S_i(R_{\Delta g}\tilde{m})$.*

Proof. Let $m = p_M(\tilde{m})$, $m' = p_M(R_{\Delta g}\tilde{m})$. So, for some strip map ϕ of (M, X, F, G, p) and some $\bar{g}K \in F$, $\tilde{m} = (\phi(x, \bar{g}K), e_i(m), \phi_x A_i(\bar{g}K))$. Letting $\bar{e}_i = pe_i(m)$, it follows that $\tilde{m} = \Phi((x, \bar{e}_i), (\bar{g}K, A_i(\bar{g}K)))$, and hence that

$$R_{\Delta g}(\tilde{m}) = \Phi((x, \bar{e}_i), (\bar{g}gK, A_i(\bar{g}gK))) = (\phi(x, \bar{g}gK), e_i(m'), \phi_x A_i(\bar{g}gK)).$$

Thus we have

$$(*): R_{\Delta g}(\phi(x, \bar{g}K), e_i(m), \phi_x A_i(\bar{g}K)) = (\phi(x, \bar{g}gK), e_i(m'), \phi_x(\bar{g}gK)),$$

with $pe_i(m) = pe_i(m') = \bar{e}_i$. (Note that $m = \phi(x, \bar{g}K)$ and $m' = \phi(x, \bar{g}gK)$.) It follows immediately from the definition of the coordinates s_i in terms of the strip maps of $\mathfrak{B}(M)$ that $pe_i(m) = pe_i(m')$ implies $s_i \circ R_{\Delta g} = s_i$ for all i (for, if $\bar{e}_i = \Sigma c_{ij}\mathfrak{a}_j$, then $e_i(m) = \Sigma c_{ij}\mathfrak{a}_j{}'(m)$ and $e_i(m') = \Sigma c_{ij}\mathfrak{a}_j{}'(m')$). Thus equation $(*)$ shows that $R_{\Delta g} S_i = S_i$, since the x_j, y_j, t_j coordinates of $R_{\Delta g}(\tilde{m})$ can be seen to depend only on the x_j, y_j, t_j coordinates of $\tilde{m}$, not on the s_j coordinates of $\tilde{m}$.

LEMMA 3. *There exists a connection ω on $(B, B(X), \Delta(G), \Delta(G), \pi)$ satisfying:*

(a) $\omega(S_i(m)) = 0$ *for all i and all $m \in B$;*

(b) $R_{r \oplus \epsilon}\omega = \omega$ *($r \oplus \epsilon$ in $O(X) \oplus \Delta(K)$, $\epsilon = \Delta$ (identity element of G)).*

Proof. A preliminary concept of horizontality H_0 on B with respect to the bundle $(B, B(X), \Delta(G), \Delta(G), \pi)$ can be defined by $H_0 S_i = S_i$, $H_0 T_i = 0$, $H_0 Y_i = 0$; this is independent of the coordinates. Let $V_0 = I - H_0$, I the identity. Note that $H_0 X_i$ is undefined.

Let H be a connection (concept of horizonality) on B with respect to the bundle $(B, X, O(X) \times \Delta(G), O(X) \times \Delta(G), p_X \circ \pi)$; let $\hat{V} = I - \hat{H}$. For any tangent vector Z at a point of B, define HZ and VZ as follows:

1. $VZ = V_o(VZ)$
2. $HZ = Z - VZ.$

So HZ and VZ are well-defined, and $VZ = V_oZ$ if Z is an S_i, T_i, or Y_i.

To prove that H is a connection on $(B, B(X), \Delta(G), \Delta(G), \pi)$, it must be shown that $R_{\Delta g}Z$ is H-horizontal for any $\Delta g \in \Delta(G)$ and any H-horizontal vector Z on B. So suppose Z is H-horizontal. Then Z is either $\hat{H}$-horizontal, or it is a linear combination of S_i's, or both. If Z is $\hat{H}$-horizontal, then $V(R_{\Delta g}Z) = V_o(VR_{\Delta g}Z) = 0$ since $R_{\Delta g}$ preserves $\hat{H}$-horizontality; and if Z is a linear combination of S_i's, Lemma 2 shows that $V(R_{\Delta g}Z) = V_o(\hat{V}(R_{\Delta g}Z)) = V_o(R_{\Delta g}Z) = 0$.

Thus H is a connection; let ω be the 1-form of H. Then $\omega(S_i) = 0$, and it must still be shown that $R_{r\oplus\epsilon}{}^*\omega = \omega$. So suppose Z is a tangent vector at a point $\tilde{m} = (m, e_i, f_i)$ of B. Let $x = pm$, and let ϕ be a strip map of (M, X, F, G, p) with $m = \phi(x, f)$; choose vectors $\bar{f}_i$ at f with $\phi_x\bar{f}_i = f_i$. Let Φ be the strip map of $(B, B(X), \Delta(G), \Delta(G)\pi)$ associated with ϕ, and define p_ϕ by: $p_\phi(\phi(x', f'), e_i', \phi_x f_i') = (f', f_i')$, for any point $(\phi(x', f'), e_i', \phi_x f_i')$. Then $\omega(Z)$ is the invariant vector field on $\Delta(G)$ whose value at the point $p_\phi(\tilde{m})$ is $p_\phi V(Z)$. Now every $R_{r\oplus\epsilon}$ maps H-horizontal vectors into H-horizontal vectors, and V-vertical vectors into V-vertical vectors (since $\pi \circ R_{r\oplus\epsilon} = R_r \circ \pi$). Thus $R_{r\oplus\epsilon} \circ V = V \circ R_{r\oplus\epsilon}$. Furthermore, $p_\phi \circ R_{r\oplus\epsilon} = p_\phi$. Thus $\omega(R_{r\oplus\epsilon}Z) = p_\phi V R_{r\oplus\epsilon}Z = p_\phi R_{r\oplus\epsilon} VZ = p_\phi VZ = \omega(Z)$.

Let ω_X be a connection on $\mathfrak{B}(X)$ with curvature form Ω_X, and let ω be a connection on $(B, B(X), \Delta(G), \Delta(G), \pi)$ which satisfies the two properties of Lemma 3; let Ω be the curvature form of ω. Define $\omega^*(\operatorname{ad}\Omega_F)$, $\omega^*(\operatorname{ad}\Omega_F)$ and $\Omega^*(\operatorname{ad}\omega_f)$ in the following way: $\omega^* \operatorname{ad}\omega_F(Z) = \operatorname{ad}\omega_F(\omega Z)$, $\omega^* \operatorname{ad}\Omega_F(Z, Z') = \operatorname{ad}\Omega_F(\omega Z, \omega Z')$, and $\Omega^* \operatorname{ad}\omega_F(Z, Z') = \operatorname{ad}\omega_F(\Omega(Z, Z'))$. These are well-defined, since the canonical connection of the second kind $\operatorname{ad}\omega_F$, and its curvature form $\operatorname{ad}\Omega_F$, are invariant under left-translations by $\Delta(G)$.

THEOREM 1. *$\bar{\omega} = \pi^*\omega_X \oplus \omega^* \operatorname{ad}\omega_F$ is a connection on $\mathfrak{B}(M)$. Its curvature form is $\bar{\Omega} = \pi^*\Omega_X \oplus (\omega^* \operatorname{ad}\Omega_F + \Omega^* \operatorname{ad}\omega_F)$.*

Proof. First, it must be shown that $\bar{\omega}$ behaves correctly under right-translations by $O(X) \oplus \Delta(K)$. So let I be the unit matrix of $O(X)$, and $r \oplus \Delta$ any element of $O(X) \oplus \Delta(K)$. Since $\pi \circ R_{r\oplus\Delta} = R_r \circ \pi$ and $\omega \circ R_{r\oplus\epsilon} = \omega$, and since ω_X and $\operatorname{ad}\omega_F$ are themselves connections, we have

$$\begin{aligned} R_{r\oplus\Delta}{}^*\bar{\omega} &= \omega_X(\pi R_{r\oplus\Delta}) \oplus \operatorname{ad}\omega_F(\omega R_{r\oplus\Delta}) = \omega_X(R_r\pi) \oplus \operatorname{ad}\omega_F(\omega R_{I\oplus\Delta}) \\ &= \omega_X(R_r\pi) \oplus \operatorname{ad}\omega_F(\operatorname{ad}\Delta^{-1}\omega) = \omega_X(R_r\pi) \oplus \operatorname{ad}\omega_F(R_\Delta\omega) \\ &= \operatorname{ad} r^{-1}(\omega_X \circ \pi) \oplus \operatorname{ad}\Delta^{-1}(\operatorname{ad}\omega_F \circ \omega) = \operatorname{ad}(r \oplus \Delta)^{-1}\bar{\omega}. \end{aligned}$$

Next, let $\phi^M(m, r \oplus \Delta) = \tilde{m}$ be a point of B, and let $\tilde{A} \oplus B$ be an element of the Lie algebra of $O(X) \oplus \Delta(K)$ with value $\alpha \oplus \beta$ at the point $r \oplus \Delta$. It must be shown that $\bar{\omega}(\phi_m{}^M(\alpha \oplus \beta)) = \tilde{A} \oplus \tilde{B}$. So let ϕ, ϕ^X, ϕ^F be the strip maps whose existence is guaranteed by Lemma 1, and let $\tilde{x}$, x, f be the points of $B(X)$, X, F satisfying $\pi(\tilde{m}) = \tilde{x}$ and $\phi(x,f) = p_M(\tilde{m})$; let $m = p_M(\tilde{m})$. Since $\phi_m{}^M(\alpha \oplus 0)$ is a linear combination of (H-horizontal) S_i's, it follows that $V\phi_m{}^M(\alpha \oplus \beta) = \phi_m{}^M(0 \oplus \beta)$. Thus:

$$\begin{aligned}\bar{\omega}(\phi_m{}^M(\alpha \oplus \beta)) &= \omega_X(\pi\phi_m{}^M(\alpha \oplus \beta)) \oplus \operatorname{ad}\omega_F(\omega\phi_m{}^M(\alpha \oplus \beta))\\ &= \omega_X(\pi\phi(\phi_x{}^X(\alpha), \phi_f{}^F(\beta)) \oplus \operatorname{ad}\omega_F(\omega\phi_m{}^M(0 \oplus \beta))\\ &= \omega_X(\phi_x{}^X(\alpha)) \oplus \operatorname{ad}\omega_F(\omega\phi(0, \phi_f{}^F(\beta)) = \omega_X(\phi_x{}^X(\alpha)) \oplus \operatorname{ad}\omega_F(\lambda),\end{aligned}$$

where λ is the left-invariant vector field on $\Delta(G)$ whose value at f is $\phi_f{}^F(\beta)$. Since ω_X and $\operatorname{ad}\omega_F$ are connections, it follows that $\bar{\omega}(\phi_m{}^M(\alpha \oplus \beta)) = \tilde{A} \oplus \tilde{B}$.

Thus, $\bar{\omega}$ is a connection on $\mathfrak{B}(M)$.

The equation of structure gives the following expression for $\bar{\Omega}$:

$$\begin{aligned}\bar{\Omega} &= d\bar{\omega} + (\tfrac{1}{2})\bar{\omega} \wedge \bar{\omega}\\ &= (d\pi^*\omega_X \oplus d\omega^* \operatorname{ad}\omega_F) + (\tfrac{1}{2})(\pi^*\omega_X \wedge \pi^*\omega_X \oplus \operatorname{ad}\omega_F \wedge \omega^* \operatorname{ad}\omega_F)\\ &= (\pi^* d\omega_X + (\tfrac{1}{2})\pi^*\omega_X \wedge \pi^*\omega_X) \oplus (d\omega^* \operatorname{ad}\omega_F + (\tfrac{1}{2})\omega^* \operatorname{ad}\omega_F \wedge \omega^* \operatorname{ad}\omega_F)\\ &= (\pi^*\Omega_X) \oplus (\omega^* \operatorname{ad}\Omega_F + (d \circ \omega^* - \omega^* \circ d)\operatorname{ad}\omega_F).\end{aligned}$$

Let Ω be the curvature form of ω; then $\Omega^* = d \circ \omega^* - \omega^* \circ d$ (see [2]), and so Theorem 1 is proved.

Thus $\bar{\omega}$ is a connection on the frame bundle of M. If K is connected, $\Delta(K)$ is contained in the rotation group $R(n)$; and so if ω_X is chosen to be a connection on the bundle of oriented frames of X, then $\bar{\omega}$ is a connection on the bundle of oriented frames of M.

If G/K is any reductive homogeneous space (that is, G is a Lie group and there exists a complement $\mathfrak{m}$ to the Lie algebra of K in the Lie algebra of G), then one can proceed as follows: Let B_X, B_F be the bundles of bases of X, F; and let B_M' be the set of all elements $(m, e_1, \cdots, e_N, f_1, \cdots, f_n)$, with $m \in M$, $e_1, \cdots, e_N$ a set of linearly independent tangent vectors at m which are horizontal (with respect to (M, X, F, G, p)), and $f_1, \cdots, f_n$ a set of linearly independent vertical tangent vectors at m. Then, on the bundle (B_M', B_X, B_F, G, π)—G acts in the natural way—ω is defined as before; however, this bundle is not a principal bundle, and so, strictly speaking, ω is not a connection. If ω_X is a connection on the bundle of bases of X, and if Ω^* denotes $d \circ \omega^* - \omega^* \circ d$, then $\bar{\omega} = \pi^*\omega_X \oplus \omega^* \operatorname{ad}\omega_F$ is a connection on the bundle of bases of M, with curvature form $\bar{\Omega} = \pi^*\Omega_X \oplus (\omega^* \operatorname{ad}\Omega_F + \Omega^* \operatorname{ad}\omega_F)$. In this case, of course, $\operatorname{ad}\omega_F$ is a connection on B_F.

The characteristic ring of *M*. From now on, K will be assumed to be connected.

Define tensors $T_r{}^X$, $T_r{}^F$, and $T_r{}^M$, on $O(X)$, $O(F)$, and $O(M)$ as follows:

(a) $T_r{}^X(A,\cdots,C) = \Sigma\epsilon a_{i_1j_1}\cdots c_{i_rj_r}$ ($A = (a_{ij}),\cdots,C = (c_{ij})$ *are* r $N\times N$ skew-symmetric matrices; $i_1,\cdots,i_r$ is any set of r numbers from among $1,\cdots,N$; $j_1,\cdots,j_r$ is any permutation of $i_1,\cdots,i_r$; ϵ is the sign of the permutation; and the summation extends over all such permutations, and all choices of $i_1,\cdots,i_r$.)

(b) $T_r{}^F(A,\cdots,C) = \Sigma\epsilon a_{i_1j_1}\cdots c_{i_rj_r}$ ($A,\cdots,C$ are r $n\times n$ skew-symmetric matrices; $i_1,\cdots,i_r$ is any set of r numbers from among $1,\cdots,n$)

(c) $T_r{}^M(A,\cdots,C) = \Sigma\epsilon a_{i_1j_1}\cdots c_{i_rj_r}$ ($A,\cdots,C$ are r $v\times v$ skew-symmetric matrices, v the dimension of M; $i_1,\cdots,i_r$ is any set r numbers from among $1,\cdots,v$.)

Then $\bar{T}_r{}^X(\Omega_X,\cdots,\Omega_X)$, $\bar{T}_r{}^F(\Omega_F,\cdots,\Omega_F)$, and $\bar{T}_r{}^M(\bar{\Omega},\cdots,\bar{\Omega})$ are $2r$-forms on $B(X)$, $\Delta(G)$, and B (the bars denote alternation with respect to the vector arguments). They define differential forms $P_r{}^X$, $P_r{}^F$, and $P_r{}^M$ on X, F, and M, with $p_X{}^*P_r{}^X = \bar{T}_r{}^X(\Omega_X,\cdots,\Omega_X)$, $p_FP_r{}^F = \bar{T}_r{}^F(\Omega_F,\cdots,\Omega_F)$, and $p_M{}^*P_r{}^M = \bar{T}_r{}^M(\bar{\Omega},\cdots,\bar{\Omega})$. A fundamental theorem of Weil shows that these differential forms are independent of the choice of connections on $\mathfrak{B}(X)$, $\mathfrak{B}(F)$, and $\mathfrak{B}(M)$.

Definition. $P_r{}^X$, $P_r{}^F$, $P_r{}^M$ are the $2r$*-th Pontrjagin characteristic forms* of X, F, and M.

LEMMA 4.

$$\begin{aligned}&\bar{T}_r{}^M(\bar{\Omega},\cdots,\bar{\Omega})\\ &\quad = \Sigma_j\bar{T}_j{}^X(\pi^*\Omega_X,\cdots,\pi^*\Omega_X)\\ &\qquad\qquad \wedge\, \bar{T}_{r-j}{}^F(\omega^*\operatorname{ad}\Omega_F + \Omega^*\operatorname{ad}\omega_F,\cdots,\omega^*\operatorname{ad}\Omega_F + \Omega^*\operatorname{ad}\omega_F).\end{aligned}$$

Proof. This is a direct consequence of Theorem 1.

Interpretation of

$$\boldsymbol{\bar{T}_r{}^F(\omega^*\operatorname{ad}\Omega_F + \Omega^*\operatorname{ad}\omega_F,\cdots,\omega^*\operatorname{ad}\Omega_F + \Omega^*\operatorname{ad}\omega_F)}.$$

M' gives rise to a space B' in a manner analogous to the manner in which M gave rise to the space B. We can consider G as a homogeneous space G/e; then G is a bundle over G/e, with fibre e, and we consider the following horizontal orthonormal left-invariant vector fields on G (note that all vector fields on G are horizontal, since the fibre is e): $X_1, \cdots, X_n$ are to be horizontal at every point with respect to the connection ω_F of $(G, G/K, K, K, \delta)$; $X_{n+1}, \cdots, X_m$— m the dimension of G—are to be vertical at every point, with respect to ω_F. Clearly, $\Delta(G) = G \times e$ for the bundle $(G, G/e, e, e, I)$; hence $(B', B(X), G, G, \pi')$, π' the natural projection of B' onto $B(X)$, is the bundle which corresponds to the bundle

$$(B, B(X), \Delta(G), \Delta(G), \pi).$$

Let p_M' be the natural projection of B' onto M'. If we choose $X_1, \cdots, X_n$ to be the same vector fields on G as the ones which defined $\Delta(G)$ in the case of the bundle $(B, G/K, K, K, \delta)$, we get a natural mapping P_o of B' into B: Let ϕ be a strip map of (M, X, F, G, p), ϕ' and Φ the associated strip maps of (M', X, G, G, p') and $(B, B(X), \Delta(G), \Delta(G), \pi)$, and Φ' the strip map of $(B', B(X), G, G, \pi')$ associated with ϕ'. Then let $P_o(\Phi'(b(x), g)) = \Phi(b(x), \Delta g)$, $b(x) \in B(X)$ and $g \in G$.

Note. Another way of defining this mapping is the following: If $\bar{m}' = (m', e_1', \cdots, e_N', f_1', \cdots, f_n', f_{n+1}', \cdots, f_m')$ is a point of B', then $P_o(\bar{m}')$ is the point $(Pm', Pe_1', \cdots, Pe_N', Pf_1', \cdots, Pf_n')$.

The following diagram is commutative $(P \circ p_M' = p_M \circ P_o)$:

$$\begin{tikzcd}
B & B' \arrow[l, "P_o"'] \arrow[d, "p_M'"] \\
M \arrow[from=u, "p_M"'] & M' \arrow[l, "P"]
\end{tikzcd}$$

One can construct a connection ω' on $(B', B(X), G, G, \pi')$ in a manner analogous to the construction of ω in Lemma 3. Then it can easily be seen that there is a connection ω on $(B, B(X), \Delta(G), \Delta(G), \pi)$ which satisfies the conditions of Lemma 3 and which satisfies the further condition: $P_o{}^*\omega = \Delta \circ \omega'$. It follows from the equation of structure that $P_o{}^*\Omega = \Delta \circ \Omega'$.

Hereafter, the connections ω and ω' will remain fixed, chosen as in the preceding paragraph.

Let $s_1 = \omega^* \operatorname{ad} \Omega_F + \Omega^* \operatorname{ad} \omega_F$. Then s_1 is $\bar{H}$-horizontal on B, and $R_{r \oplus \Delta}{}^* s_1 = \operatorname{ad}(r \oplus \Delta)^{-1} s_1$, $r \oplus \Delta \in O(X) \oplus \Delta(K)$.

Let S_1 be the following linear-transformation valued 2-form on M: If t, t' are tangent vectors at a point m of M, and if T, T' are tangent vectors at a point $(m, e_1, \cdots, e_N, f_1, \cdots, f_n)$ of B with $p_M T = t$ and $p_M T' = t'$, then $S_1(t,t')$ is the linear transformation of the tangent space to M at m whose matrix with respect to the basis $e_1,\cdots,e_N,f_1,\cdots,f_n$ is $s_1(T,T')$.

Thus $\bar{T}_r^F(s_1,\cdots,s_1)=p_M{}^*\bar{T}_r^F(S_1,\cdots,S_1)$.

LEMMA 5. *Let* $s_2=\omega'^*\Omega_F+\Omega'^*\omega_F$. *Then* $P_o{}^*s_1=\Delta\circ s_2$.

Proof. $P_o{}^*s_1=P_o{}^*(\omega^*\operatorname{ad}\Omega_F+\Omega^*\operatorname{ad}\omega_F)=\operatorname{ad}\Omega_F(\omega\circ P_o)+\operatorname{ad}\omega_F(\Omega\circ P_o)$ $=\operatorname{ad}\Omega_F(\Delta\circ\omega')+\operatorname{ad}\omega_F(\Delta\circ\Omega')=\Delta(\Omega_F\omega'+\omega_F\Omega')=\Delta\circ s_2$. (The second-to-last equality follows from the definition of the connection $\operatorname{ad}\omega_F$ in terms of ω_F and Δ.)

Definition. T_r^F defines a tensor t_r^F on K in the following way: If $X,\cdots,Z$ are r elements of the Lie algebra of K, then $t_r^F(X,\cdots,Z)$ $T_r^F(\operatorname{ad}X[\mathfrak{m}],\cdots,\operatorname{ad}Z[\mathfrak{m}])$ (recall that the Lie algebra of G splits, with respect to the fundamental bilinear form, into the direct sum of the Lie algebra of K and its orthogonal complement $\mathfrak{m}$.) Since K is connected, t_r^F is invariant under K.

Now each tensor t_r^F gives rise to a characteristic form p_r^F of M with respect to the bundle (M',M,K,K,p). We have:

LEMMA 6. *The forms* $\bar{T}_r^F(S_1,\cdots,S_1)$ *and* p_r^F *are cohomologous on* M.

Proof. It will be shown that there is a curvature form $\bar{\Omega}$ on the bundle (M',M,K,K,P) for which $p^*\bar{T}_r^F(S_1,\cdots,S_1)=\bar{t}_r^F(\bar{\Omega},\cdots,\bar{\Omega})$; this will prove the lemma. It is equivalent, however, to show that $p_M{}'^*\bar{t}_r^F(\bar{\Omega},\cdots,\bar{\Omega})$ $=P_o{}^*\bar{T}_r^F(s_1,\cdots,s_1)$. Now it follows from Lemma 5 that $P_o{}^*\bar{T}_r^F(s_1,\cdots,s_1)$ $=\bar{t}_r^F(s_2,\cdots,s_2)$, since $\Delta(Z)=\operatorname{ad}Z[\mathfrak{m}]$ for any Z in the Lie algebra of K; hence it must be shown that $p_M{}'^*\bar{t}_r^F(\bar{\Omega},\cdots,\bar{\Omega})=\bar{t}_r^F(s_2,\cdots,s_2)$. We will now prove, in fact, that $\bar{\Omega}$ can be so chosen that $p_M{}'^*\bar{\Omega}=s_2$.

We define a connection H'' on (M',X,G,G,p') by the condition $p_M{}'\circ H'$ $=H''\circ p_M{}'$, This is well-defined; and if ω'' is the 1-form of H'', it will be shown in the following paragraph that $\omega'=p_M{}'^*\omega''$. Thus the equation of structure shows that $\Omega'=p_M{}'^*\Omega''$. Now $\omega_F\circ\omega''$ is a connection on the bundle (M',M,K,K,P); let $\bar{\Omega}$ be its curvature form. Then it follows from the equation of structure that $\bar{\Omega}=\omega''^*\Omega_F+\Omega''^*\omega_F$. Thus

$$p_M{}'^*\bar{\Omega}=\omega'^*\Omega_F+\Omega'^*\omega_F=s_2.$$

Proof that $\omega'=p_M{}'^*\omega''$. Let ϕ be a strip map of (M,X,F,G,p), let ϕ' be the associated strip map of (M,X,G,G,p'), and let Φ be the associated strip map of $(B,B(X),\Delta(G),\Delta(G),\pi)$; let Φ' be the strip map of $(B',B(X),G,G,\pi')$ associated with ϕ'.

(a) $p_M' \circ V' = V'' \circ p_M'$ (where $H' + V' = I$ and $H'' + V'' = I$). For any vector Y of B',

$$p_M'H'Y + p_M'V'Y = p_M'Y = H''p_M'Y + V''p_M'Y = p_M'H'Y + V''p_M'Y,$$

hence $p_M'V'(Y) = V''p_M'(Y)$.

(b) Let $b(x)$ be a point of $B(X)$ and g a point of G; then

$$p_M'\Phi'(b(x), g) = p_M'(\phi'(x, g), e_i, \phi_x'A_i(g)) = \phi'(x, g),$$

(c) $\phi_x'^{-1} \circ p_M' = \Phi_{b(x)}'^{-1}$ on $\pi'^{-1}(b(x))$. Let $\tilde{m}' = \Phi'(b(x), g)$ be a point of B'. So $\Phi_{b(x)}'^{-1}(\tilde{m}') = g$, and it follows from (b) that $\phi_x'^{-1}p_M'(\tilde{m}') = \phi_x'^{-1}(\phi'(x, g)) = g$.

We now show that $\omega' = \omega'' \circ p_M'$ on H'-horizontal and H'-vertical vectors of B', thus completing the proof. If Z is H'-horizontal, then $\omega'(Z) = \omega''(p_M'Z) = 0$. If Z is H'-vertical, it follows from (a) that $p_M'Z$ is H''-vertical; thus, if Z lies in the fibre above the point $b(x)$ of $B(X)$, it follows from (c) that $\omega''(p_M'Z) = \phi_x'^{-1}p_M'(V'Z) = \Phi_{b(x)}'^{-1}(V'Z) = \omega'(V'Z)$ (where, of course, the two middle terms are extended to left-invariant vector fields).

THEOREM 2. *For any positive integer* r, $P_r^M = \Sigma_j p^*P_j^X \wedge p_{r-j}^F$, *where* P_r^M, P_j^X *are the Pontrjagin forms of* M, X, *and where* p_{r-j}^F *is the characteristic form on* M *defined by the tensor* t_{r-j}^F *on* K.

Proof. $\bar{T}_j^X(\Omega_X, \cdots, \Omega_X) = p_X^*P_j^X$, where p_X is the projection of $B(X)$ onto X; thus $\pi^*(\bar{T}_j^X(\Omega_X, \cdots, \Omega_X)) = \pi^*p_X^*P_j^X$. Now $p_X \circ \pi = p \circ p_M$; and so it follows from Theorem 1 and Lemma 6 that:

$$p_M^*P_r^M = \bar{T}_r^M(\bar{\Omega}, \cdots, \bar{\Omega}) = \Sigma_j\, p_M^*p^*P_j^X \wedge p_M^*p_{r-j}^F = p_M^*(\Sigma_j\, p^*P_j^X \wedge p_{r-j}^F).$$

Thus $P_r^M = \Sigma_j\, p^*P_j^X \wedge p_{r-j}^F$.

Remark. The bundle (M', M, K, K, p) and the mapping Δ of K into $O(n)$ induce a principal bundle over M with fibre and group $O(n)$. So p_r^F is the $2r$-th Pontrjagin form of M with respect to this bundle. It is known that the Pontrjagin forms of degree greater than $2n$ of a principal bundle with group $O(n)$ are zero; bundle; hence $p_s^F = 0$ if $s > 2n$.

COROLLARY. *If the characteristic ring of* M *with respect to the bundle* (M', M, K, K, P) *is empty, then*:

(a) $P_r^M = p^*P_r^X$ *if* $r \leqq$ *dimension of* X;

(b) $P_r^M = 0$ *if* $r >$ *dimension of* X.

This holds in particular when K *is a normal subgroup of* G.

Proof. Only the second part of this corollary remains to be proved. If K is a normal subgroup of G, let f be a cross-section of G/K into G, and let f' be the following mapping of M into M': $f'(\phi(x, gK)) = \phi'(x, f(gK))$. So f' is defined in terms of strip maps, but is clearly independent of the strip map used; it is a cross-section of M into M', and hence the characteristic ring of M with respect to the bundle (M', M, K, K, P) is empty.

PRINCETON UNIVERSITY.

REFERENCES.

[1] W. Ambrose and I. M. Singer, "A theorem on holonomy," *Transactions of the American Mathematical Society*, vol. 75 (1943), pp. 428-443.

[2] H. Cartan, *Colloque de Topologie* (*espaces fibrés*), Bruxelles, 1950, Liège et Paris, 1951, pp. 15-27 and 57-71.

[3] S. S. Chern, *Topics in Differential Geometry*, Institute for Advanced Study, Princeton, 1951 (mimeographed notes).

ON MAPS FROM SPHERES TO EUCLIDEAN SPACES.*

By Chung-Tao Yang.

---

1. Introduction. Knaster [1] proposed the following problem: Given a map (= continuous function) f of an $(m+n-2)$-sphere S^{m+n-2} into the euclidean n-space and m distinct points $x_1, \cdots, x_m$ of S^{m+n-2}, does there exist a rotation r of S^{m+n-2} such that $f(r(x_1)) = \cdots = f(r(x_m))$? Up to the present we know only several partial solutions of this problem. For the case $n = 2$, a positive answer follows from the generalized Borsuk-Ulam's theorem by Hopf [2]. If $m = 3$, $n = 1$ and x_1, x_2, x_3 are end points of three mutually orthogonal radii, a positive answer can be found in Kakutani [3]. The result of Kakutani was extended by both Yamabe-Yujobô [4] and Floyd [5]. The former removed the restriction on m and the latter removed the restriction on x_1, x_2, x_3. The purpose of this note is to extend the result of Kakutani by removing the restriction on n and weakening the restriction on x_1, x_2, x_3. In fact, we shall prove

Theorem 1. *Given a number d, $0 < d \leqq 2\pi/3$, and a map f of an $(n+1)$-sphere S^{n+1} into the euclidean n-space, there exist three points x_1, x_2, x_3 of S^{n+1} such that $f(x_1) = f(x_2) = f(x_3)$ and the spherical distance between any two of x_1, x_2, x_3 is equal to d.*

Notice that Theorem 1 and Floyd [5] give a strong indication that for the case $m = 3$ the answer to Knaster's problem is probably in the affirmative. The proof of Theorem 1 is roughly as follows. Let X_d be the subset of $S^{n+1} \times S^{n+1} \times S^{n+1}$ consisting of all the elements (x_1, x_2, x_3) such that the spherical distance between any two of x_1, x_2, x_3 is equal to d. If there is a map f of S^{n+1} into the euclidean n-space such that for no $(x_1, x_2, x_3) \in X_d$, $f(x_1) = f(x_2) = f(x_3)$, we shall construct a map g of X_d into a $(2n-1)$-sphere S^{2n-1} and a subset Y of X_d which is topologically a cylinder with the Stiefel manifold $V_{n+1,2}$ as its base. Then we arrive at a contradiction by proving that g is essential when restricted on one base of Y but is inessential when restricted on the other. For the case $n = 1$, Y consists of two circular

---

* Received May 8, 1957.

cylinders. If Y is replaced by either of these two cylinders, the proof we have is essentially the same as that in [3].

As in [2], the same proof yields a generalized theorem concerning maps from Riemannian manifolds to euclidean spaces.

2. Preliminaries. Throughout this note, n denotes a positive integer and R^n denotes the euclidean n-space. Let S^{n+1} be an $(n+1)$-sphere with center o. Whenever $x, y \in S^{n+1}$, $\rho(x, y)$ denotes the spherical distance between x and y, i.e., the angle between the vectors ox and oy. Clearly ρ is a Riemannian metric on S^{n+1} and geodesics are arcs of great circles of S^{n+1}. If x_1, x_2, x_3 are three distinct points of S^{n+1} such that $\rho(x_2, x_3) = \rho(x_3, x_1) = \rho(x_1, x_2) = d$, then $0 < d \leqq 2\pi/3$.

For any fixed number d, $0 < d \leqq 2\pi/3$, we let X_d be the subset of $S^{n+1} \times S^{n+1} \times S^{n+1}$ consisting of all the elements (x_1, x_2, x_3) such that $\rho(x_2, x_3) = \rho(x_3, x_1) = \rho(x_1, x_2) = d$. The elements of X_d are called *d-triples* on S^{n+1}.

If $d < 2\pi/3$, there is a natural homeomorphism between X_d and the Stiefel manifold $V_{n+2,3}$ consisting of all the orthogonal 3-frames with o as the origin. In fact, any $(x_1, x_2, x_3) \in X_d$ determines an orthogonal 3-frame (oy, oy_2, oy_3) as follows. oy_1 is the unit vector on ox_1. oy_2 is the unit vector on the 2-plane $[ox_1x_2]$ orthogonal to oy_1 and such that the projection of ox_2 on oy_2 is positive. oy_3 is the unit vector on the 3-plane $[ox_1x_2x_3]$ orthogonal to the 2-plane $[ox_1x_2]$ and such that the projection of ox_3 on oy_3 is positive. The correspondence $(x_1, x_2, x_3) \to (oy_1, oy_2, oy_3)$ is clearly a desired homeomorphism. If $d = 2\pi/3$, then for every $(x_1, x_2, x_3) \in X_d$, x_1, x_2, x_3 are on a great circle of S^{n+1}. Therefore x_3 is on the 2-plane $[ox_1x_2]$ and is determined by x_1, x_2. Just as above, the d-triple (x_1, x_2, x_3) determines an orthogonal 2-frame (oy_1, oy_2) and the correspondence $(x_1, x_2, x_3) \to (oy_1, oy_2)$ gives a homeomorphism of $X_{2\pi/3}$ onto the Stiefel manifold $V_{n+2,2}$ consisting of all the orthogonal 2-frames with o as the origin.

The function $T\colon X_d \to X_d$ defined by $T(x_1, x_2, x_3) = (x_2, x_3, x_1)$ is a periodical transformation of period 3 and has no fixed point.

Let p be a point of S^{n+1} and let S^n be the n-sphere contained in S^{n+1} consisting of all the points x with $\rho(p, x) = \cos^{-1}((1 + 2\cos d)/3)^{\frac{1}{2}}$. It is easily seen that every d-triple (x_1, x_2, x_3) on S^{n+1} with $\rho(p, x_1) = \rho(p, x_2) = \rho(p, x_3)$ is a $(2\pi/3)$-triple on S^n and conversely every $(2\pi/3)$-triple on S^n is a d-triple on S^{n+1}. Hence all the $(2\pi/3)$-triples on S^n form a subset A_p of X_d. The set A_p is homeomorphic to the Stiefel manifold $V_{n+1,2}$ and is invariant under the periodical transformation T. For $n > 1$, A_p is connected; but for $n=1$, A_p consists of two components each of which is homeomorphic to a circle and is invariant under T.

Let I be the unit closed interval $[0,1]$. Then a map $h\colon A_p\times I\rightarrow X_d$ can be constructed as follows. Given any $(x_1,x_2,x_3)\in A_p$ we let Π be the n-plane perpendicular to the 2-plane $[opx_1]$ at o. Let (px_1) be the geodesic on S^{n+1} joining p and x_1, i.e., the shorter arc of the great circle $S^{n+1}\cap[opx_1]$ with end points p, x_1. For each $t\in I$ we denote by σ_t the rotation of S^{n+1} around Π such that $\sigma_t(x_1)$ is the point of (px_1) with $\rho(x_1,\sigma_t(x_1))=t\rho(p,x_1)$. Now we define $h\colon A_p\times I\rightarrow X_d$ by $h((x_1,x_2,x_3),t)=(\sigma_t(x_1),\sigma_t(x_2),\sigma_t(x_3))$. Clearly h is a homeomorphism of $A_p\times I$ into X_d, $h(A_p\times 0)=A_p$ and $B_p=h(A_p\times 1)$ consists of all the d-triples (x_1,x_2,x_3) on S^{n+1} with $x_1=p$.

3. Proof of Theorem 1. Suppose that Theorem 1 is false, i.e., there is a map f of S^{n+1} into R^n and a number d, $0<d<2\pi/3$, such that for no $(x_1,x_2,x_3)\in X_d$, $f(x_1)=f(x_2)=f(x_3)$. Then a map g of X_d into a $(2n-1)$-sphere S^{2n-1} can be constructed as follows. For any $(x_1,x_2,x_3)\in X_d$ we let

$$f(x_1)=(\alpha_1,\cdots,\alpha_n),\quad f(x_2)=(\alpha_{n+1},\cdots,\alpha_{2n}),\quad f(x_3)=(\alpha_{2n+1},\cdots,\alpha_{3n});$$

$$\beta_i=\alpha_i-(\alpha_i+\alpha_{n+i}+\alpha_{2n+i})/3,$$

$$\beta_{n+i}=\alpha_{n+i}-(\alpha_i+\alpha_{n+i}+\alpha_{2n+i})/3\qquad \beta_{2n+i}=\alpha_{2n+i}-(\alpha_i+\alpha_{n+i}+\alpha_{2n+i})/3,\qquad i=1,\cdots,n;$$

$$\gamma_i=\beta_i/\Big(\sum_{k=1}^{3n}\beta_k^2\Big)^{\frac{1}{2}},\qquad i=1,\cdots,3n.$$

Notice that our assumption implies that $\alpha_i=\alpha_{n+i}=\alpha_{2n+i}$ does not hold for all $i=1,\cdots,n$. Therefore $\sum_{k=1}^{3n}\beta_k^2>0$ and hence γ are well-defined. Let S^{2n-1} be the $(2n-1)$-sphere in R^{3n} given by

$$u_1^2+\cdots+u_{3n}^2=1,\qquad u_i+u_{n+i}+u_{2n+i}=0,\qquad i=1,\cdots,n,$$

where $u_1,\cdots,u_{3n}$ are coordinates of points in R^{3n}. Then $g(x_1,x_2,x_3)=(\gamma_1,\cdots,\gamma_{3n})$ gives a map g of X_d into S^{2n-1}.

The map $T\colon S^{2n-1}\rightarrow S^{2n-1}$ defined by

$$T(u_1,\cdots,u_n,u_{n+1},\cdots,u_{3n})=(u_{n+1},\cdots,u_{3n},u_1,\cdots,u_n)$$

is a periodical transformation of period 3 and has no fixed point. Moreover $gT=Tg$.

Let p be a point of S^{n+1} where the first coordinate of $f(p)$ attains its least upper bound. Let A_p and B_p be as in the preceding section. Then for any $(x_1, x_2, x_3) \in B_p$, $g(x_1, x_2, x_3) = (\gamma_1, \cdot \cdot \cdot, \gamma_{3n})$ must satisfy $\gamma_1 \geqq \gamma_{n+1}$. Therefore $g(B_p)$ is a proper subset of S^{2n-1} and hence $g|B_p$, i.e., the map g restricted on B_p, is inessential. As seen in the preceding section, A_p and B_p may be regarded as bases of a cylinder contained in X_d. Hence, if we can show that $g|A_p$ is essential, we arrive at a contradiction which completes the proof of Theorem 1.

4. Special homology theory. In order to prove that $g|A_p$ is essential, we need the following special case of the special homology theory of Smith. Let X be a compact Hausdorff space and let T be a periodical transformation of X which is of period 3 and has no fixed point. Let ρ, ρ' stand for $1 - T$, $1 + T + T^2$ or vice versa. As seen in [6], we have, for each integer $k \geqq 0$, a (Čech) homology group $H_k(X)$ and two special homology groups $H_k^\rho(X)$ and $H_k^{\rho'}(X)$, where the group Z_3 of integers mod 3 is used as coefficient group. We also have homomorphisms

$$\partial \colon H_{k+1}^\rho(X) \to H_k^{\rho'}(X), \quad i \colon H_k^{\rho'}(X) \to H_k(X), \quad j \colon H_k(X) \to H_k^\rho(X).$$

(4.1) *Let* X, T, ∂, i, j *be as above. Then the sequence*

$$H_0^\rho(X) \xleftarrow{j} H_0(X) \xleftarrow{i} H_0^{\rho'}(X) \xleftarrow{\partial} \cdot \cdot \cdot$$

$$\longleftarrow H_{k-1}^{\rho'}(X) \xleftarrow{\partial} H_k^\rho(X) \xleftarrow{j} H_k(X) \xleftarrow{i} H_k^{\rho'}(X) \xleftarrow{\partial} H_{k+1}^\rho(X) \longleftarrow \cdot \cdot \cdot$$

is exact. [6]

(4.2) *Let* X, T, ∂, i, j *be as above and let* Y, T, ∂, i, j *be their analogies. Then for any map* $g \colon X \to Y$ *with* $gT = Tg$ *there are induced homomorphisms*

$$g \colon H_k(X) \to H_k(X), \quad g \colon H_k^\rho(X) \to H_k^\rho(X), \quad g \colon H_k^{\rho'}(X) \to H_k^{\rho'}(X)$$

such that the diagram

$$\begin{tikzcd}
H_k^\rho(X) \arrow[d, "g"] & H_k(X) \arrow[l, "j"'] \arrow[d, "g"] & H_k^{\rho'}(X) \arrow[l, "i"'] \arrow[d, "g"] & H_{k+1}^\rho(X) \arrow[l, "\partial"'] \arrow[d, "g"] \\
H_k^\rho(Y) & H_k(Y) \arrow[l, "j"'] & H_k^{\rho'}(Y) \arrow[l, "i"'] & H_{k+1}^\rho(Y) \arrow[l, "\partial"']
\end{tikzcd}$$

is commutative. [6]

As a consequence of (4.1) we have:

(4.3) *Let X, T, ∂, i, j be as above. If for some integer $m > 0$, $H_k(X)$ is equal to Z_3 or 0 according as $k = 0$, m or not, then $H_k{}^{\rho}(X) = 0$ or Z_3 according as $k > m$ or not. Moreover $i\colon H_m{}^{\rho'}(X) \to H_m(X)$, $j\colon H_0(X) \to H_0{}^{\rho}(X)$ and $\partial\colon H_{k+1}{}^{\rho}(X) \to H_k{}^{\rho'}(X)$, $k = 0, \cdots, m-1$, are isomorphisms onto.* [6]

5. Continuation of the proof of Theorem 1. Now we return to the proof of Theorem 1 and assert that $g|A_p$ is essential. Since the homomorphism of homology groups induced by an inessential map is always trivial, we have only to prove

(5.1) *The homomorphism $g\colon H_{2n-1}(A_p) \to H_{2n-1}(S^{2n-1})$ induced by the map $g|A_p$ is not trivial.*

Suppose that n is even. Then $H_k(A_p)$ is the same as $H_k(S^{2n-1})$ which is equal to Z_3 or 0 according as $k = 0$, $2n-1$ or not [7]. By (4.3), all the horizontal homomorphisms in the diagram

$$\begin{tikzcd}
H_0(A_p) \arrow[r, "j"] \arrow[d, "g"] & H_0{}^{\rho}(A_p) \arrow[d, "g"] & H_1{}^{\rho'}(A_p) \arrow[l, "\partial"'] \arrow[d, "g"] & H_2{}^{\rho}(A_p) \arrow[l, "\partial"'] \arrow[d, "g"] \\
H_0(S^{2n-1}) \arrow[r, "j"] & H_0{}^{\rho}(S^{2n-1}) & H_1{}^{\rho'}(S^{2n-1}) \arrow[l, "\partial"'] & H_2{}^{\rho}(S^{2n-1}) \arrow[l, "\partial"']
\end{tikzcd}$$

$$\begin{tikzcd}
{} & \cdots \arrow[l, "\partial"'] & H_{2n-1}{}^{\rho}(A_p) \arrow[l, "\partial"'] \arrow[r, "i"] \arrow[d, "g"] & H_{2n-1}(A_p) \arrow[d, "g"] \\
{} & \cdots \arrow[l, "\partial"'] & H_{2n-1}{}^{\rho'}(S^{2n-1}) \arrow[l, "\partial"'] \arrow[r, "i"] & H_{2n-1}(S^{2n-1})
\end{tikzcd}$$

are isomorphisms onto. Since A_p and S^{2n-1} are both connected, $g\colon H_0(A_p) \to H_0(S^{2n-1})$ is an isomorphism onto. Hence, by (4.2), all the vertical homomorphisms are isomorphisms onto. In particular,

$$g\colon H_{2n-1}(A_p) \to H_{2n-1}(S^{2n-1})$$

is not trivial.

Suppose that $n = 1$. Then A_p consists of two components and each of the components is topologically a circle invariant under T. It is easily seen that the proof above remains true when A_p is replaced by either of its components. Hence for $n = 1$, $g\colon H_{2n-1}(A_p) \to H_{2n-1}(S^{2n-1})$ is also not trivial. Notice that this is essentially the proof in [3].

Suppose now that n is an odd number > 1. Since A_p consists of all the $(2\pi/3)$-triples on S^n, it contains a subset A_p' consisting of all the $(2\pi/3)$-triples on an $(n-1)$-sphere S^{n-1}. As seen in Section 2, A_p' is homeomorphic to the Stiefel manifold $V_{n,2}$ and therefore $H_k(A_p')$ is equal to Z_3 or 0 according as $k = 0,\ 2n-3$ or not. Therefore in the diagram

$$\begin{tikzcd}
H_0(A_p') \arrow[r, "j"] \arrow[d] & H_0^{\rho}(A_p') \arrow[d] & H_1^{\rho'}(A_p') \arrow[l, "\partial"'] \arrow[d] & \cdots \arrow[l, "\partial"'] & H_{2n-3}^{\rho'}(A_p') \arrow[l, "\partial"'] \arrow[d] \\
H_0(S^{2n-1}) \arrow[r, "j"] & H_0^{\rho}(S^{2n-1}) & H_1^{\rho'}(S^{2n-1}) \arrow[l, "\partial"'] & \cdots \arrow[l, "\partial"'] & H_{2n-3}^{\rho'}(S^{2n-1}) \arrow[l, "\partial"']
\end{tikzcd}$$

all the horizontal homomorphisms are isomorphisms onto and among the vertical homomorphisms which are induced by the map $g|A_p'$, the first one on the left is an isomorphism onto. Hence, by (4.3), all the vertical homomorphisms are isomorphisms onto. Let I be the image of $H_{2n-3}^{\rho'}(A_p')$ in $H_{2n-3}^{\rho'}(A_p)$ under the homomorphism induced by the inclusion map. Then g maps I isomorphically onto $H_{2n-3}^{\rho}(S^{2n-1})$.

If $n > 3$, it is known [7] that $H_{2n-3}(A_p)$ and $H_{2n-2}(A_p)$ are both 0. Therefore, by (4.1), $\partial\colon H_{2n-2}^{\rho}(A_p) \to H_{2n-3}^{\rho'}(A_p)$ is an isomorphism onto and hence

$$I \subset \partial H_{2n-2}^{\rho}(A_p). \tag{5.2}$$

If $n = 3$, A_p is a sphere bundle over S^3 with respect to the projection $(x_1, x_2, x_3) \to x_1$. Since the projection induces an isomorphism of $H_3(A_p)$ onto $H_3(S^3)$ and maps A_p' into S^2, it follows that $i\colon H_3^{\rho'}(A_p) \to H_3(A_p)$ maps I into 0. Hence (5.2) also holds for $n = 3$.

Now we observe the diagram

$$\begin{tikzcd}
 & H_{2n-2}^{\rho}(A_p) \arrow[dl, "g\partial"'] \arrow[d, "g"] & H_{2n-1}^{\rho'}(A_p) \arrow[l, "\partial"'] \arrow[r, "i"] \arrow[d, "g"] & H_{2n-1}(A_p) \arrow[d, "g"] \\
H_{2n-3}^{\rho'}(S^{2n-1}) & H_{2n-2}^{\rho}(S^{2n-1}) \arrow[l, "\partial"'] & H_{2n-1}^{\rho'}(S^{2n-1}) \arrow[l, "\partial"'] \arrow[r, "i"] & H_{2n-1}(S^{2n-1})
\end{tikzcd}$$

It is easily seen that $i\colon H_{2n-1}^{\rho'}(A_p) \to H_{2n-1}(A_p)$ is an isomorphism onto. Since $n \geqq 3$, $H_{2n-2}(A_p) = 0$. It follows from (4.1) that $\partial\colon H_{2n-1}^{\rho'}(A_p) \to H_{2n-2}^{\rho}(A_p)$ is an isomorphism onto. Since, by (4.3), all the homomorphisms of the lower row are isomorphisms and since

$$g\partial H_{2n-2}^{\rho'}(A_p) \supset gI \neq 0,$$

we infer from (4.2) that $g\colon H_{2n-1}(A_p) \to H_{2n-1}(S^{2n-1})$ is not trivial. This completes the proof of (5.1) and hence Theorem 1 is proved.

6. A generalization. As in [2], Theorem 1 can be extended to a theorem on compact Riemannian manifolds without singularity.

Let M be a Riemannian manifold without singularity. For any point a of M and any unit tangent vector v at a there is a geodesic beginning at a and tangent to v. We shall denote by (a, v, e) the point of M obtained by moving a point along the geodesic a distance e from a.

THEOREM 2. *Let M be a compact $(n+1)$-dimensional Riemannian manifold without singularity and let f be a map of M into the euclidean n-space. Then for any $e > 0$ there exists a point a of M and three unit tangent vectors v_1, v_2, v_3 of M at a such that the angle between any two of v_1, v_2, v_3 is equal to $2\pi/3$ and $f(a, v_1, e) = f(a, v_2, e) = f(a, v_3, e)$.*

The proof of Theorem 2 is the same as that of Theorem 1 except for a few modifications. Let V be the totality of (a, v_1, v_2, v_3), where a is a point of M and v_1, v_2, v_3 are unit tangent vectors at a such that the angle between any two of them is equal to $2\pi/3$. If Theorem 2 is false, then there is a map $f\colon M \to R^n$ and a number $e > 0$ such that for no $(a, v_1, v_2, v_3) \in V$, $f(a, v_1, e) = f(a, v_2, e) = f(a, v_3, e)$. Therefore we may construct a map $g\colon V \to S^{2n-1}$ as in the proof of Theorem 1. Since M is compact, there is a point p of M where the first coordinate of $f(p)$ attains its least upper bound. Let A_p be the subset of V consisting of all the elements (a, v_1, v_2, v_3) with $a = p$. As (5.1), the map $g \mid A_p$ is essential. For any $(a, v_1, v_2, v_3) \in A_p$ and $t \in I$ we define $(a(t), v_1(t), v_2(t), v_3(t)) \in V$ such that $a(t) = (p, -v_1, te)$ and $v_1(t)$, $v_2(t)$, $v_3(t)$ are parallel displacements of v_1, v_2, v_3 along the geodesic $a(s)$, $0 \leqq s \leqq t$. Then

$$((a, v_1, v_2, v_3), t) \to (a(t), v_1(t), v_2(t), v_3(t))$$

defines a map h of $A_p \times I$ into V with

$$h((a, v_1, v_2, v_3), 0) = (a, v_1, v_2, v_3).$$

Since $h(A_p \times 1)$ consists of all the elements (a, v_1, v_2, v_3) with $p = (a, v_1, e)$, it follows that the map g restricted on $B_p = h(A_p \times 1)$ is inessential. Hence we arrive at a contradiction.

Theorem 2 is a generalization of Theorem 1, because the former becomes the latter if M is an $(n+1)$-sphere with the spherical distance function as its Riemannian metric and $e = \cos^{-1}((1 + 2\cos d)/3)^{\frac{1}{2}}$.

UNIVERSITY OF PENNSYLVANIA.

REFERENCES.

[1] B. Knaster, *Colloquium Mathematicum*, vol. 1 (1947), pp. 30-31.

[2] H. Hopf, "Verallgemeinerung bekannter Abildungs- und Überdeckungssätze," *Portugaliae Mathematica*, vol. 4 (1944), pp. 129-139.

[3] S. Kakutani, "A proof that there exists a circumscribing cube around any bounded closed convex set in R^3," *Annals of Mathematics*, vol. 43 (1942), pp. 739-741..

[4] H. Yamabe and Z. Yujobô, "On the continuous functions defined on a sphere," *Osaka Mathematical Journal*, vol. 2 (1950), pp. 19-22.

[5] E. E. Floyd, "Real-valued mappings of spheres," *Proceedings of the American Mathematical Society*, vol. 6 (1955), pp. 957-959.

[6] ———, "On periodic maps and the Euler characteristics of associated spaces," *Transactions of the American Mathematical Society*, vol. 72 (1952), pp. 138-147.

[7] E. Stiefel, "Richtungsfelder und Fernparallelismus in n-dimensionalen Mannigfaltigkeiten," *Commentarii Mathematici Helvetici*, vol. 8 (1936), pp. 3-51.

A FORMULA FOR SEMISIMPLE LIE GROUPS.*

By Harish-Chandra.

---

1. Introduction. Let G be a connected semisimple Lie group and $\mathcal{E}$ the set of all equivalence classes of irreducible unitary representations of G. Let T_ω denote the character of any class $\omega \in \mathcal{E}$ (see [4(a)]). Then the Plancherel formula for G is equivalent to the following statement. *There exists a unique positive measure $d\omega$ on $\mathcal{E}$ (called the Plancherel measure) such that*

$$f(1) = \int_{\mathcal{E}} T_\omega(f)\,d\omega$$

for all[1] $f \in C_c^\infty(G)$. Let δ denote the Dirac measure on G corresponding to the unit mass at 1 so that $\delta(f) = f(1)$. Then the above formula may also be interpreted in the form

$$\delta = \int_{\mathcal{E}} T_\omega d\omega.$$

Let T be a distribution and D a differential operator on G. Then, for any $x, y \in G$, we define the distribution $T' = xTy$ and the differential operator $D' = xDy$ as follows. $T'(f) = T(f')$ and $D'f = Df'$ $(f \in C_c^\infty(G))$, where $f'(z) = f(xzy)$ $(z \in G)$. Also, put $xT = xTy$, $Tx = yTx$, for $y = 1$. T is called invariant if $xTx^{-1} = T$ for all $x \in G$. Let $\mathfrak{Z}$ be the algebra of those differential operators D for which $D = xDy$ $(x, y \in G)$. We say that T is an eigen-distribution of $\mathfrak{Z}$ if it is an eigen-distribution for every D in $\mathfrak{Z}$. Let Z be the center of G. Then T is an eigen-distribution of Z if zT is a numerical multiple of T for every $z \in Z$. It is known (see[4(a)]) that the characters T_ω $(\omega \in \mathcal{E})$ are invariant and that they are eigen-distributions of both $\mathfrak{Z}$ and Z. Hence the Plancherel formula may be regarded as an "expansion" of δ in terms of such invariant eigen-distributions.

Although the existence and uniqueness of the Plancherel measure are known, so far no general method of computing it has been found. The object of this paper is to give a formula which can be regarded as a first step towards the determination of $d\omega$. Let G' and S, respectively, denote the sets

---

* Received December 4, 1956.

[1] See footnote 1 of [4(g)] for certain notational conventions.

of regular and singular elements in G (see [4(c)]). Consider a Cartan subgroup A of G and let $\mathfrak{H}$ denote the algebra of those differential operators on A which are invariant under all translations of A. Then for any $f \in C_c^\infty(G)$, we shall define a function Ψ_f on $A' = A \cap G'$ of class C^∞ in such a way that the following conditions hold.[2]

(1) If $f' = xfx^{-1}$ $(x \in G, f \in C_c^\infty(G))$, then $\Psi_f = \Psi_{f'}$.

(2) There exists a homomorphism γ of $\mathfrak{Z}$ into $\mathfrak{H}$ such that $\Psi_{zf} = \gamma(z)\Psi_f$ for all $z \in \mathfrak{Z}$ and $f \in C_c^\infty(G)$.

(3) For every $u \in \mathfrak{H}$ and $f \in C_c^\infty(G)$, $u\Psi_f$ remains bounded on A' and Ψ_f vanishes outside some compact subset of A.

(4) The mapping $f \rightarrow \Psi_f$ is continuous in a suitable sense (see Theorem 2).

Let l be the rank of G. Then $A \cap S$ is the union of a finite number of closed subgroups of A of dimension $l - 1$. (3) implies that $u\Psi_f$ has no singularities (on A) except possible jumps across $A \cap S$. Let $\hat{A}$ be the character group of A and $T_{\hat{a}}(f)$ the value of the Fourier transform of Ψ_f at $\hat{a} \in \hat{A}$. Then it follows from (1) and (4) that $T_{\hat{a}}$ is an invariant distribution on G (see Lemma 17). Moreover, since $Z \subset A$, it is clear that $T_{\hat{a}}$ is an eigen-distribution of Z. For any function $\phi \in C_c^\infty(A)$, let $\tilde{\phi}$ denote the Fourier transform of ϕ. Then it is clear that, for any $u \in \mathfrak{H}$, there exists an analytic function $\hat{u}$ on $\hat{A}$ such that $(u\phi)^\sim = \hat{u}\tilde{\phi}$ $(\phi \in C_c^\infty(A))$. Let $\chi_{\hat{a}}(z)$ $(z \in \mathfrak{Z}, \hat{a} \in \hat{A})$ denote the value of $(\gamma(z))^\wedge$ at $\hat{a}$. Then if Ψ_f could be extended to a function of class C^∞ on A, it would follow from (2) that

$$T_{\hat{a}}(zf) = \chi_{\hat{a}}(z)\ T_{\hat{a}}(f).$$

Hence except for the above-mentioned jumps, $T_{\hat{a}}$ would have been an eigen-distribution of $\mathfrak{Z}$.

Let $l_-(A)$ denote the dimension of the maximal compact subgroup of A/Z. We say that A is fundamental if $l_-(A)$ has the maximum possible value. If A is fundamental, we can select an open neighborhood B of 1 in A and a connected component A_1 of $B \cap A'$ such that 1 lies in the closure of A_1 and the following additional condition holds.

(5) There exists an element $u_0 \in \mathfrak{H}$ such that

$$f(1) = \operatorname*{Lim}_{a \to 1} (u_0\Psi_f)(a) \qquad (a \in A_1) \tag{I}$$

for all $f \in C_c^\infty(G)$.

---

[2] $\Psi_f = \epsilon_+ F_f \prod_{\alpha \in P} |\eta_\alpha|^{\frac{1}{2}}$ in the notation of Lemma 18.

Let us agree, for a moment, to ignore the complications due to the jumps. Then (5) implies the formula

$$\text{(II)} \qquad f(1) = \int_{\hat{A}} \hat{u}_0(\hat{a}) T_{\hat{a}}(f)\, d\hat{a} \qquad (f \in C_c^\infty(G)),$$

where $d\hat{a}$ is the (suitably normalized) Haar measure on $\hat{A}$. Therefore

$$\delta = \int_{\hat{A}} \hat{u}_0(\hat{a}) T_{\hat{a}}\, d\hat{a},$$

and since $T_{\hat{a}}$ are invariant eigen-distributions of Z and $\mathfrak{Z}$, we should expect this formula to be closely related to the Plancherel formula.

Let $r(G)$ be the maximum number of nonconjugate Cartan subgroups of G. In case $r(G) = 1$, it is actually true that Ψ_f can be extended to a function of class C^∞ on A for every $f \in C_c^\infty(G)$. Hence the above formula holds in this case. Moreover, it is then possible to define a mapping $\hat{a} \to \omega(\hat{a})$ of $\hat{A}$ into $\mathcal{E}$ such that $T_{\hat{a}} = cT_{\omega(\hat{a})}$, where c is a constant. Then

$$\delta = c \int_{\hat{A}} \hat{u}_0(\hat{a}) T_{\omega(\hat{a})}\, d\hat{a}$$

and, in fact this is substantially the same as the Plancherel formula for G. Thus if $r(G) = 1$, the problem of the determination of the Plancherel measure is solved completely. This is so in particular if G is either compact or complex (see [4(b)]).

Now in the general case ($r(G) > 1$), the jumps of the function Ψ_f (or its derivatives) cannot be ignored, and therefore $T_{\hat{a}}$ is no longer an eigen-distribution of $\mathfrak{Z}$. Nevertheless, there are good reasons to believe (see [4(e)]) that for suitable $\hat{a} \in \hat{A}$, $T_{\hat{a}}$ is intimately related to a character T_ω of G. Hence equation (I) may still be regarded as a first step towards the derivation of the Plancherel formula. The importance of such a relation has been clearly recognized by Gelfand and Graev [3].

Now suppose for a moment that A is compact so that $\hat{A}$ is discrete. In view of equation (II) (which, however, is not quite exact due to the jumps of Ψ_f), one would expect to get a "discrete series" (see [4(f)]) in $\mathcal{E}$ parametrized by $\hat{A}$. More precisely, we should expect the existence of a mapping which assigns to each $\hat{a}$ lying in a suitable subset $\hat{A}_0$ of $\hat{A}$, a discrete class $\omega(\hat{a})$ in $\mathcal{E}$ such that the Plancherel measure of $\omega(\hat{a})$ is $c\hat{u}_0(\hat{a})$, where c is a constant independent of $\hat{a}$. This expectation has actually been confirmed in a large number of cases (see [4(f)]).

If G is simple, its first Betti number $b(G)$ is either 0 or 1. Assuming that A is compact, we should expect to get a discrete series in both cases.

So far, a general method for constructing a discrete series has been obtained only when $b(G)=1$ (see [4(d), (e), (f)]).

This paper is divided into two parts. The main results of Part I are contained in Theorem I and the Corollary to Lemma 12. We need them in Part II in order to carry over the results of [4(h), (i)] from its Lie algebra to the group G itself. Sections 4 and 5 are devoted to the verification of the five conditions stated above. A short account of the principal results of this paper has appeared in [4(j)].

Part I.

2. Proof of Theorem 1.

Let R and C be the fields of real and complex numbers, respectively, and let G be a connected semisimple Lie group with the Lie algebra $\mathfrak{g}_0$ over R. Let $\mathfrak{h}_0$ be a Cartan subalgebra of $\mathfrak{g}_0$ and A the corresponding Cartan subgroup of G (see [4(c), § 2]). Our main object in this section is to prove the following theorem.

THEORM 1. *Let a_0 be an element in A and Ξ the centralizer of a_0 in G. Denote the natural mapping of G on the factor space $G^*=G/\Xi$ by $x\rightarrow x^*$ $(x\in G)$. Then we can find a neighborhood B of a_0 in A with the following property. Given any compact set ω in G, there exists a compact set Ω^* in G^* satisfying the condition that, if $xax^{-1}\in\omega$ for some $a\in B$ and $x\in G$, then $x^*\in\Omega^*$.*

The proof is rather long and requires considerable preparation. First we need two results on nilpotent groups. Let F be a field which is either R or C, and let N be a connected Lie group and $\mathfrak{n}$ its Lie algebra over F. (If $F=C$, we assume of course that N is a complex analytic group.) Suppose $\mathfrak{n}$ is nilpotent and $\mathfrak{n}^{(k)}$ $(k=1,2,\cdots)$ are ideals in $\mathfrak{n}$ such that $\mathfrak{n}^{(1)}=\mathfrak{n}$, $[\mathfrak{n},\mathfrak{n}^{(k)}]\subset\mathfrak{n}^{(k+1)}$ $(k\geqq 1)$ and $\mathfrak{n}^{(k)}=\{0\}$ if k is sufficiently large. Furthermore suppose $\mathfrak{n}$ can be written as a direct sum of two subspaces $\mathfrak{n}_1$, $\mathfrak{n}_2$ satisfying the following two conditions:

(1) $\mathfrak{n}_1$ is a subalgebra of $\mathfrak{n}$,

(2) $\mathfrak{n}^{(k)}=\mathfrak{n}_1\cap\mathfrak{n}^{(k)}+\mathfrak{n}_2\cap\mathfrak{n}^{(k)}$ for all $k\geqq 1$.

Then we have the following result.

LEMMA 1. *Under the above conditions every element in N can be written in the form $\exp X_2\exp X_1$, where $X_1\in\mathfrak{n}_1$ and $X_2\in\mathfrak{n}_2$.*

Without loss of generality, we may assume that N is simply connected. Then $\mathfrak{n}$ being nilpotent, the exponential mapping is a one-one regular mapping of $\mathfrak{n}$ onto N. We denote its inverse by $x \to \log x$ $(x \in N)$. X being any element in N, we shall first show that for every integer $k \geqq 0$, we can find $X_1 \in \mathfrak{n}_1$ such that

$$\log(\exp X \exp(-X_1)) \in \mathfrak{n}_2 + \mathfrak{n}^{(k+1)}.$$

We use induction on k. If $k = 0$ our assertion is true trivially. So let us suppose $k \geqq 1$. By the induction hypothesis, we can choose $Y_1 \in \mathfrak{n}_1$ such that $Z = \log(\exp X \exp(-Y_1)) \in \mathfrak{n}_2 + \mathfrak{n}^{(k)}$. Select $Z' \in \mathfrak{n}^{(k)}$ such that $Z - Z' \in \mathfrak{n}_2$. Then $Z' = Z_1 + Z_2$, where $Z_i \in \mathfrak{n}_i \cap \mathfrak{n}^{(k)}$ $(i = 1, 2)$. Hence, by the Campbell-Hausdorff formula, we get

$$\log(\exp Z \exp(-Z_1)) \equiv Z - Z_1 \bmod \mathfrak{n}^{(k+1)}.$$

Moreover, $Z - Z_1 = (Z - Z') + Z_2 \in \mathfrak{n}_2$, and therefore

$$\log(\exp X \exp(-Y_1)\exp(-Z_1)) \in \mathfrak{n}_2 + \mathfrak{n}^{(k+1)}.$$

However, $\mathfrak{n}_1$ is a nilpotent algebra, and therefore $\exp Z_1 \exp Y_1 = \exp X_1$ for some $X_1 \in \mathfrak{n}_1$. Hence $\log(\exp X \exp(-X_1)) \in \mathfrak{n}_2 + \mathfrak{n}^{(k+1)}$.

Now taking k sufficiently large, we get $X_2 = \log(\exp X \exp(-X_1)) \in \mathfrak{n}_2$, and so $\exp X = \exp X_2 \exp X_1$. This proves the lemma.

Let $X_1, \cdots, X_r$ be a base for $\mathfrak{n}$ over F such that $[X_i, X_j] \in \sum_{k>j} FX_k$ $(1 \leqq i \leqq j \leqq r)$. Put $\mathfrak{n}_{(0)} = \{0\}$, $\mathfrak{n}_{(j)} = \sum_{1 \leqq i \leqq j} FX_i$ $(1 \leqq j \leqq r)$, and let π_j denote the projection of $\mathfrak{n}$ on $\mathfrak{n}_{(j)}$ given by $\pi_j X_i = X_i$ $(1 \leqq i \leqq j)$ and $\pi_j X_i = 0$ $(j < i \leqq r)$. Let ${}_m\mathfrak{n}_{(j)}$ denote the Cartesian product of $\mathfrak{n}_{(j)}$ with itself m times.

LEMMA 2. *Suppose N is simply connected and m is a positive integer. Then for each j $(1 \leqq j \leqq r)$, there exists a polynomial mapping*[3] *p_j of ${}_m\mathfrak{n}_{(j-1)}$ into $\mathfrak{n}_{(j)}$ such that*

$$\pi_j \log(\exp Y_1 \exp Y_2 \cdots \exp Y_m)$$
$$= \pi_j(Y_1 + \cdots + Y_m) + p_j(\pi_{j-1}Y_1, \pi_{j-1}Y_2, \cdots, \pi_{j-1}Y_m)$$

for all $Y_1, \cdots, Y_m \in \mathfrak{n}$.

We shall prove this by induction on $r = \dim \mathfrak{n}$. If $r = 1$, $\mathfrak{n}$ is abelian and our statement is obvious. So now suppose $r \geqq 2$. Put $\mathfrak{n}^* = \mathfrak{n}/FX_r$ and $N^* = N/N_r$, where N_r is the one-parameter subgroup of N corresponding to X_r. Since X_r lies in the center of $\mathfrak{n}$, it is clear that $\log(\exp X \exp Y) = X + Y$ $(X \in \mathfrak{n}, Y \in FX_r)$, and therefore the exponential mapping of $\mathfrak{n}^*$ onto N^* is still one-one. Let $X \rightarrow X^*$ $(X \in \mathfrak{n})$ denote the natural mapping of $\mathfrak{n}$ on $\mathfrak{n}^*$, and let $\mathfrak{n}_{(j)}{}^*$ be the image of $\mathfrak{n}_{(j)}$ $(1 \leqq j \leqq r)$ under this mapping. Define the projection $\pi_j{}^*$ of $\mathfrak{n}^*$ on $\mathfrak{n}_{(j)}{}^*$ by $\pi_j{}^* X^* = (\pi_j X)^*$ $(X \in \mathfrak{n}, 1 \leqq j \leqq r)$. Then since $\dim \mathfrak{n}^* < \dim \mathfrak{n}$, our induction hypothesis is applicable to $\mathfrak{n}^*$. Hence for each j, there exists a polynomial mapping q_j of ${}_m\mathfrak{n}_{(j-1)}$ into $\mathfrak{n}_j$ such that

---

[3] Let U, V be two vector spaces over F of finite dimension. A mapping p of U into V is called a polynomial mapping if, for every linear function λ on V, the function $u \to \lambda(p(u))$ $(u \in U)$ is a polynomial function on U.

$$\pi_j \log(\exp Y_1 \cdots \exp Y_m)$$
$$\equiv \pi_j(Y_1 + \cdots + Y_m) + q_j(\pi_{j-1}Y_1, \cdots, \pi_{j-1}Y_m) \bmod FX_r$$

for $Y_1, \cdots, Y_m \in \mathfrak{n}$. But if $j < r$, $\mathfrak{n}_{(j)} \cap (FX_r) = \{0\}$, and therefore

$$\pi_j \log(\exp Y_1 \cdots \exp Y_m) = \pi_j(Y_1 + \cdots + Y_m) + q_j(\pi_{j-1}Y_1, \cdots, \pi_{j-1}Y_m).$$

On the other hand, if $j = r$, π_r is the identity mapping of $\mathfrak{n}$. Moreover, it is known that $(Y_1, \cdots, Y_m) \rightarrow \log(\exp Y_1 \cdots \exp Y_m)$ is a polynomial mapping of ${}_m\mathfrak{n} = {}_m\mathfrak{n}_{(r)}$ into $\mathfrak{n}$ (see Birkhoff [1]). Now put

$$p_r(Y_1, \cdots, Y_m) = \log(\exp Y_1 \cdots \exp Y_m) - (Y_1 + \cdots + Y_m).$$

Then since X_r belongs to the center of $\mathfrak{n}$, it is clear that $p_r(Y_1, \cdots, Y_m) = p_r(\pi_{r-1}Y_1, \cdots, \pi_{r-1}Y_m)$. Hence

$$\log(\exp Y_1 \cdots \exp Y_m) = (Y_1 + \cdots + Y_m) + p_r(\pi_{r-1}Y_1, \cdots, \pi_{r-1}Y_m),$$

and this proves our assertion for $j = r$.

Let $\mathfrak{g}$, $\mathfrak{h}$ be the complexifications of $\mathfrak{g}_0$, $\mathfrak{h}_0$, respectively, and let G_c be a complex analytic group with the Lie algebra $\mathfrak{g}$. From now on we shall use the notation of [4(g), (h)] without further comment. In view of the Corollary of Lemma 1 of [4(c)], we may obviously assume that $\theta(\mathfrak{h}_0) = \mathfrak{h}_0$. For each root α (of $\mathfrak{g}$ with respect to $\mathfrak{h}$), select an eleemnt $X_\alpha \neq 0$ in $\mathfrak{g}$ such that $[H, X_\alpha] = \alpha(H) X_\alpha$ for all $H \in \mathfrak{h}$. Define the set P of positive roots as in [4(h), § 5], and put $\mathfrak{n} = \sum_{\alpha \in P} CX_\alpha$. Let A_c be the analytic subgroup of G_c corresponding to $\mathfrak{h}$. If α is a root, we denote by ξ_α the corresponding character of A_c so that $\xi_\alpha(\exp H) = e^{\alpha(H)}$ $(H \in \mathfrak{h})$. Let a_0 be a fixed element in A_c and P_1 the subset of those roots $\alpha \in P$ for which $\xi_\alpha(a_0) = 1$. Then if P_2

is the complement of P_1 on P, we put $\mathfrak{n}_1 = \sum_{\alpha \in P_1} CX_\alpha$, $\mathfrak{n}_2 = \sum_{\alpha \in P_2} CX_\alpha$. Let $\alpha_1 < \alpha_2 < \cdots < \alpha_r$ be all the roots in P. Put

$$\mathfrak{n}^{(k)} = \sum_{k \leqq i \leqq r} CX_{\alpha_i} \qquad (k \geqq 1).$$

Then it is obvious that all the conditions of Lemma 1 are fulfilled. Let N_c and N_1 be the (complex) analytic subgroups of G_c corresponding to $\mathfrak{n}$ and $\mathfrak{n}_1$, respectively. Also, let N_2 denote the set of all elements in N_c of the form $\exp X$ $(X \in \mathfrak{n}_2)$. It is well known that N_c is simply connected, and therefore the exponential mapping defines an isomorphism of the complex vector space $\mathfrak{n}$ onto N_c (with respect to its structure as a complex manifold). Hence N_2 is closed in N_c.

Choose a compact neighborhood B_c of a_0 in A_c such that, if $\alpha \in P_2$, then ξ_α never takes the value 1 on B_c.

LEMMA 3. *Let Ξ_c denote the centralizer of a_0 in G_c and $x \rightarrow x^*$ the natural mapping of G_c onto $G_c^* = G_c/\Xi_c$. Then for any compact set ω_c in G_c, we can select a compact set Ω_c^* in G_c^* satisfying the following condition. If $xax^{-1} \in \omega_c$ for some $x \in G_c$ and $a \in B_c$, then $x^* \in \Omega_c^*$.*

We shall derive Theorem 1 from the above lemma. But in order to prove this lemma, we need some additional facts.

LEMMA 4. *There exist compact sets ω_1, ω_2 in N_1, N_2, respectively, having the following property. Suppose $n_2 a n_1 n_2^{-1} \in \omega_c$ for some $a \in B_c$, $n_1 \in N_1$ and $n_2 \in N_2$. Then $n_1 \in \omega_1$ and $n_2 \in \omega_2$.*

It is well known that $A_c N_c$ is closed in G_c and the mapping $(a, n) \rightarrow an$ $(a \in A_c, n \in N_c)$ of $A_c \times N_c$ into G_c is topological (see Iwasawa [5]). We define $\log n$ $(n \in N_c)$ as before and denote by t_α $(\alpha \in P)$ the Cartesian coordinates in the complex Euclidean space $\mathfrak{n}$ corresponding to the base $(X_\alpha)_{\alpha \in P}$. Then it would be enough to show that, under our assumptions, $t_\alpha(\log n_1)$ and $t_\alpha(\log n_2)$ remain bounded for every $\alpha \in P$. Put $\mathfrak{n}_\alpha = \sum_{0 < \beta < \alpha} CX_\beta$, and let π_α denote the projection of $\mathfrak{n}$ on $\mathfrak{n}_\alpha$ given by $\pi_\alpha X_\beta = X_\beta$ $(0 < \beta < \alpha)$ and $\pi X_\beta = 0$ $(\beta \geqq \alpha)$. Then from Lemma 2, there exists a polynomial function p_α on $\mathfrak{n}_\alpha \times \mathfrak{n}_\alpha \times \mathfrak{n}_\alpha$ such that

$$t_\alpha(\log(\exp X_1 \exp X_2 \exp X_3)) = t_\alpha(X_1 + X_2 + X_3) + p_\alpha(\pi_\alpha X_1, \pi_\alpha X_2, \pi_\alpha X_3)$$

for $X_1, X_2, X_3 \in \mathfrak{n}$. Now $n_2 a n_1 n_2^{-1} = a(a^{-1} n_2 a) n_1 n_2^{-1}$. Since ω_c is compact, it follows from what we have said above that if $a'n' \in \omega_c$ $(a' \in A_c, n' \in N_c)$, then $t_\alpha(\log n')$ remains bounded for every $\alpha \in P$. This shows that

$t_\alpha(\log(a^{-1}n_2an_1n^{-1}))$ must remain bounded for every $\alpha \in P$. Now suppose the assertion of the lemma is false. Then let β be the lowest root in P such that $|t_\beta(\log n_1)| + |t_\beta(\log n_2)|$ does not remain bounded when n_1, n_2 and a vary in such a way as to fulfill our assumptions. Put $X_i = \log n_i$ $(i = 1, 2)$. Then[4] $\log(a^{-1}n_2a) = \mathrm{Ad}(a^{-1})X_2$ and so it is clear that[5]

$$t_\beta(\log(a^{-1}n_2an_1n_2^{-1})) = t_\beta((\mathrm{Ad}(a^{-1}) - 1)X_2 + X_1)$$
$$+ p_\beta(\pi_\beta\mathrm{Ad}(a^{-1})X_2, \pi_\beta X_1, -\pi_\beta X_2).$$

Therefore

$$(\xi_\beta(a^{-1}) - 1)t_\beta(X_2) + t_\beta(X_1)$$
$$= t_\beta(\log(a^{-1}n_2an_1n_2^{-1})) - p_\beta(\pi_\beta\mathrm{Ad}(a^{-1})X_2, \pi_\beta X_1, -\pi_\beta X_2).$$

Now it follows from the definition of β and the compactness of B_c that the right side remains bounded. Moreover, if $\beta \in P_1$, then $t_\beta(X_2) = 0$. On the other hand, if $\beta \in P_2$, then $t_\beta(X_1) = 0$ and $(\xi_\beta(a^{-1}) - 1)^{-1} = \xi_\beta(a)(1 - \xi_\beta(a))^{-1}$ remains bounded for $a \in B_c$. Therefore, in either case, we conclude from the above equation that $|t_\beta(X_1)| + |t_\beta(X_2)|$ remains bounded. As this contradicts the definition of β, the lemma is proved.

COROLLARY. *There exists a compact set* ω^* *in* G_c^* *with the following property. If* $nan^{-1} \in \omega_c$ *for some* $n \in N_c$ *and* $a \in B_c$, *then* $n^* \in \omega^*$.

From Lemma 1, $n = n_2n_1$ $(n_2 \in N_2, n_1 \in N_1)$. Hence $nan^{-1} = n_2an_1'n_2^{-1}$, where $n_1' = a^{-1}n_1an_1^{-1}$. Choose compact sets ω_1, ω_2 corresponding to Lemma 4. Then $n_2 \in \omega_2$. Moreover, since $N_1 \subset \Xi_c$, it follows that $n^* = n_2^* \in \omega_2^*$. Hence we can take $\omega^* = \omega_2^*$.

Now we come to the proof of Lemma 3. Let U be the real analytic subgroup of G_c corresponding to the compact real form $\mathfrak{u} = \mathfrak{k}_0 + (-1)^{\frac{1}{2}}\mathfrak{p}_0$ of $\mathfrak{g}$. Then U is compact and it is well known (see Iwasawa [5]) that $G = UA_cN_c = UN_cA_c$. This implies that $G_c = UN_2N_1A_c$. Moreover $\Xi_c \supset N_1A_c$. Now suppose $xax^{-1} \in \omega_c$ $(x \in G_c, a \in B_c)$. Then if $x = un_2n_1a'$ $(u \in U, n_2 \in N_2, n_1 \in N_1, a' \in A_c)$ and $n_1' = a^{-1}n_1an_1^{-1}$, we have

$$xax^{-1} = u(n_2an_1'n_2^{-1})u^{-1} \in \omega_c.$$

Therefore $n_2an_1'n_2^{-1} \in U\omega_cU$. Since $U\omega_cU$ is also compact, we can select sets ω_1, ω_2 in accordance with Lemma 4, corresponding to $U\omega_cU$. Then $n_2 \in \omega_2$ and $x \in U\omega_2N_1A_c \subset U\omega_2\Xi_c$. Hence $x^* \in \Omega_c^*$, where $\Omega_c^* = (U\omega_2)^*$. This completes the proof of Lemma 3.

---

[4] As usual $x \to \mathrm{Ad}(x)$ $(x \in G)$ denotes the adjoint representation.

[5] Here 1 stands for the identity mapping of $\mathfrak{g}$.

We now return to Theorem 1. Let Z be the center of G. Since $Z \subset \Xi$, it is clear that, for the proof of this theorem, we may replace G by any other connected group locally isomorphic to it. Let us therefore assume that G is the real analytic subgroup of G_c corresponding to $\mathfrak{g}_0$. Also, it will be convenient to suppose that G_c is simply connected. Let η be the conjugation of $\mathfrak{g}$ with respect to $\mathfrak{g}_0$. Then η can be "extended" to a (real) automorphism of G_c which we again denote by η. Since G is the connected component of the subgroup consisting of those points of G_c which are left fixed by η, G is closed in G_c. Also $A = A_c \cap G$ (see [4(c), § 2]) and $\Xi = G \cap \Xi_c$. Therefore $G^* = G/\Xi$ may be regarded as a subset of G_c^*. It is clear that Theorem 1 would follow immediately from Lemma 3 if we can show that G^* is closed in G_c^* and the inclusion mapping of G^* into G_c^* is topological. An elementary argument shows that this mapping is certainly continuous. Hence it is sufficient to prove the following result.

LEMMA 5. *Let $\{x_r^*\}_{r \geqq 1}$ be a sequence in G^* which converges in G_c^* to some point x^*. Then $x^* \in G^*$ and x_r^* converges to x^* in G^*.*

Define the structure of a Hilbert space on $\mathfrak{g}$ by means of the positive-definite Hermitian form $\| X \|^2 = -B(X, \bar{\theta}(X))$ $(X \in \mathfrak{g})$ as in [4(h), § 5] For any linear transformation T on $\mathfrak{g}$, put $\| T \|^2 = \mathrm{sp}(T^*T)$, where T^* is the adjoint of T. Then $\| X \| = \| \mathrm{ad}\, X \|$ $(X \in \mathfrak{g})$. We write $\| x \| = \| \mathrm{Ad}(x) \|$ $(x \in G_c)$ and call a subset ω' of G_c bounded if $\| x \|$ remains bounded for $x \in \omega'$. Since the center of G_c is finite, it is clear that ω' is bounded if and only if its closure in G_c is compact. Select points $x_r \in G$ and $x \in G_c$ lying in the cosets x_r^* and x^*, respectively. Then obviously $x_r a_0 x_r^{-1} \to x a_0 x^{-1}$ in G_c, and therefore $\| x_r a_0 x_r^{-1} \|$ remains bounded. But as we shall show below (Lemma 6) this implies that x_r^* are all contained in a compact subset of G^*, and from this, the assertion of Lemma 5 follows immediately. Thus it remains to prove the following lemma.

LEMMA 6. *Let ω be a compact set in G. Then there exists a compact subset Ω^* of G^* satisfying the condition that if $x a_0 x^{-1} \in \omega$ $(x \in G)$, then $x^* \in \Omega^*$.*

Let $\mathfrak{z}_0$ be the centralizer of a_0 in $\mathfrak{g}_0$. Then it follows from Lemma 7 of [4(c)] that $\theta(\mathfrak{z}_0) = \mathfrak{z}_0$, and therefore (see [4(h), Lemma 10]) $\mathfrak{z}_0$ is reductive in $\mathfrak{g}_0$. Moreover $\mathfrak{h}_0 \subset \mathfrak{z}_0$, and therefore the ranks of $\mathfrak{g}_0$ and $\mathfrak{z}_0$ are the same. *Now it is convenient to drop our earlier notation and redefine $\mathfrak{h}_{\mathfrak{p}_0}$ and $\mathfrak{h}_0$ as follows.* Let $\mathfrak{h}_{\mathfrak{p}_0}$ be a maximal abelian subspace of $\mathfrak{z}_{\mathfrak{p}_0} = \mathfrak{z}_0 \cap \mathfrak{p}_0$. We extend it to a Cartan subalgebra $\mathfrak{h}_0$ of $\mathfrak{z}_0$. Then $\mathfrak{h}_0 = \mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{h}_{\mathfrak{k}_0}$, where

$\mathfrak{h}_{\mathfrak{k}_0} = \mathfrak{h}_0 \cap \mathfrak{k}_0$, and since the ranks of $\mathfrak{g}_0$ and $\mathfrak{z}_0$ are equal and $\mathfrak{z}_0$ is reductive in $\mathfrak{g}_0$, $\mathfrak{h}_0$ is also a Cartan subalgebra of $\mathfrak{g}_0$. We now introduce the notation[6] of [4(h), § 5] corresponding to the *new* $\mathfrak{h}_0$. In particular, A is now the Cartan subgroup of G corresponding to $\mathfrak{h}_0$ and $A_\mathfrak{p} = \exp \mathfrak{h}_{\mathfrak{p}_0}$. Since $\mathfrak{h}_0$ is contained in the centralizer of a_0, it is obvious that $a_0 \in A$. Let $a_0 = a_1 a_2$, where $a_1 \in A \cap K$ and $a_2 \in A_\mathfrak{p}$ (see [4(c), Lemma 7]). Clearly $\mathfrak{m}_{\mathfrak{p}_0}$ and $\mathfrak{n}_0$ are invariant under $\mathrm{Ad}(a_0)$. Moreover, since $\mathfrak{h}_{\mathfrak{p}_0}$ is maximal abelian in $\mathfrak{z}_{\mathfrak{p}_0}$, $\mathfrak{z}_{\mathfrak{p}_0} \cap \mathfrak{m}_{\mathfrak{p}_0} = \{0\}$. Therefore $\mathrm{Ad}(a_0)$ can never take the eigenvalue 1 in $\mathfrak{m}_{\mathfrak{p}_0}$. Put $\mathfrak{n}_0' = \mathfrak{z}_0 \cap \mathfrak{n}_0$ and let $\mathfrak{n}_0''$ be the orthogonal complement of $\mathfrak{n}_0'$ in $\mathfrak{n}_0$. Since $\mathrm{Ad}(a_1)$ is unitary and $\mathrm{Ad}(a_2)$ is self-adjoint and they commute, it follows that both $\mathfrak{n}_0'$ and $\mathfrak{n}_0''$ are invariant under $\mathrm{Ad}(a_0)$ and no eigenvalue of $\mathrm{Ad}(a_0)$ in $\mathfrak{n}_0''$ can be 1. The same argument shows that $\mathfrak{z}_{\mathfrak{p}_0}$ and $\mathfrak{m}_{\mathfrak{p}_0}$ are mutually orthogonal.

Now let $\mathfrak{z}$, $\mathfrak{m}_\mathfrak{p}$, $\mathfrak{h}$, $\mathfrak{n}'$, $\mathfrak{n}''$, $\mathfrak{n}$, $\mathfrak{g}_\lambda$ $(\lambda \in \mathfrak{F})$ denote the complexifications of $\mathfrak{z}_0$, $\mathfrak{m}_{\mathfrak{p}_0}$, $\mathfrak{h}_0$, $\mathfrak{n}_0'$, $\mathfrak{n}_0''$, $\mathfrak{n}_0$, $\mathfrak{g}_{0\lambda}$, respectively, in $\mathfrak{g}$ and similarly for the others. Since every element in $\mathrm{ad}(\mathfrak{h}_{\mathfrak{p}_0})$ is self-adjoint, both $\mathfrak{n}'$, $\mathfrak{n}''$ are invariant under $\mathrm{ad}(\mathfrak{h}_\mathfrak{p})$. Put $\mathfrak{n}_\lambda' = \mathfrak{n}' \cap \mathfrak{g}_\lambda$, $\mathfrak{n}_\lambda'' = \mathfrak{n}'' \cap \mathfrak{g}_\lambda$ $(\lambda \in \mathfrak{F})$. Then $\mathfrak{n}_\lambda'$ and $\mathfrak{n}_\lambda''$ are mutually orthogonal and invariant under $\mathrm{Ad}(a_0)$, and $\mathfrak{n}' = \sum_{\lambda>0} \mathfrak{n}_\lambda'$, $\mathfrak{n}'' = \sum_{\lambda>0} \mathfrak{n}_\lambda''$, where both sums are orthogonal. Moreover, $\mathrm{Ad}(a_0)$ never takes the eigenvalue 1 on $\mathfrak{n}_\lambda''$, while its restriction on $\mathfrak{n}'$ is the identity. Choose a base for $\mathfrak{g}_\lambda$ $(\lambda > 0)$ consisting of eigen-vectors of $\mathrm{Ad}(a_0)$. Then every element of this base lies either in $\mathfrak{n}_\lambda'$ or in $\mathfrak{n}_\lambda''$. Moreover, all these bases, put together for all $\lambda > 0$, form a base $(X_1, \cdots, X_q)$ for $\mathfrak{n}$. We number the elements X_i in such a way that if $X_i \in \mathfrak{g}_\lambda$, $X_j \in \mathfrak{g}_\mu$ and $0 < \lambda < \mu$, then $i < j$. Then it is obvious that $[X_i, X_j] \in \sum_{k>j} CX_k$ $(1 \leqq i < j \leqq q)$.

Let N, N', respectively, be the analytic subgroups of G corresponding to $\mathfrak{n}_0$, $\mathfrak{n}_0'$ and put $N'' = \exp \mathfrak{n}_0''$. Define M and $M_\mathfrak{p} = \exp \mathfrak{m}_{\mathfrak{p}_0}$ as in [4(h), § 5]. Then from Lemma 11 of [4(h)], $G = KM_\mathfrak{p}NA_\mathfrak{p}$, and it is obvious that $\Xi \supset N'A_\mathfrak{p}$. Moreover, it follows from Lemma 1 that $N = N''N'$. Finally, since G is imbedded in the complex group G_c, the center of G is finite, and therefore K is compact. Therefore, we may assume without loss of generality that $\omega = K\omega K$. Now suppose $x = kmna$ $(k \in K, m \in M_\mathfrak{p}, n \in N, a \in A_\mathfrak{p})$ and $xa_0x^{-1} \in \omega$. Then $(mna)a_0(mna)^{-1} \in \omega$, and therefore

$$a_0^{-1} y a_0 y^{-1} = a_0^{-1} mna_0 n^{-1} m^{-1} \in a_0^{-1}\omega,$$

---

[6] **Unless it is explicitly stated otherwise, the various symbols $\mathfrak{m}_0$, $\mathfrak{m}_{\mathfrak{p}_0}$, $\mathfrak{n}_0$, $\mathfrak{g}_{0\lambda}$ $(\lambda \in \mathfrak{F})$** etc. are always meant to have the same meaning as in [4(h), § 5] corresponding to the *new* $\mathfrak{h}_0$.

where $y = mna$. On the other hand,

$$a_0^{-1}mna_0n^{-1}m^{-1} = (a_0^{-1}ma_0)\,m^{-1}m\,(a_0^{-1}na_0n^{-1})\,m^{-1}$$

and $(a_0^{-1}ma_0)m^{-1} \in M_{\mathfrak{p}}M_{\mathfrak{p}} \subset M \subset KM_{\mathfrak{p}}$ while $m(a_0^{-1}na_0n^{-1})m^{-1} \in mNm^{-1} = N$. Therefore, since $a_0^{-1}\omega$ is compact, it follows from Lemma 11 of [4(h)] that both $\| a_0^{-1}ma_0m^{-1} \|$ and $\| m(a_0^{-1}na_0n^{-1})m^{-1} \|$ must remain bounded (as x varies in G subject to the condition that $xa_0x^{-1} \in \omega$). However, as we shall see in Lemma 7, the boundedness of $\| a_0^{-1}ma_0m^{-1} \|$ implies that m remains within a compact subset of $M_{\mathfrak{p}}$. Since $\| m^{-1}zm \| \leqq \| m^{-1} \| \, \| z \| \, \| m \|$ for any $z \in G$, it follows that $\| a_0^{-1}na_0n^{-1} \|$ also remains bounded. Now let $n = n_2n_1$ $(n_1 \in N', n_2 \in N'')$. Then $a_0^{-1}na_0n^{-1} = a_0^{-1}n_2a_0n_2^{-1}$. But as we shall prove in Lemma 9, the boundedness of $\| a_0^{-1}n_2a_0n_2^{-1} \|$ implies the boundedness of $\| n_2 \|$. Then if $x_1 = kmn_2$, we have $x^* = x_1^*$ and $\| x_1 \| = \| mn_2 \| \leqq \| m \| \, \| n_2 \|$. This shows that x_1 stays within a bounded subset of G, and therefore $x^* = x_1^*$ within a compact subset of G^*. Hence our assertion is now proved.

We have still to prove the two results which were used above.

LEMMA 7. *Suppose m varies in $M_{\mathfrak{p}}$ in such a way that $\| ma_0m^{-1} \|$ remains bounded. Then $\| m \|$ also remains bounded.*

Define a_1, a_2 as above. Then $a_0 = a_1a_2$ and a_2 commutes with every element in $M_{\mathfrak{p}}$ since $[\mathfrak{h}_{\mathfrak{p}_0}, \mathfrak{m}_{\mathfrak{p}_0}] = \{0\}$. Therefore $ma_0m^{-1} = (ma_1m^{-1})a_2$, and so $\| ma_1m^{-1} \|$ remains bounded. Moreover, the exponential mapping being one-one and regular on $\mathfrak{p}_0$, we may denote by log its inverse on $\exp \mathfrak{p}_0$. Then it would be sufficient to show that $\| \log m \|$ remains bounded. For this we need the following lemma.

LEMMA 8. *Let k be an element in K. Then if $n = \dim_C \mathfrak{g}$,*

$$\| pkp^{-1} \| \geqq n^{\frac{1}{2}} \cosh(n^{-\frac{3}{2}} \| \log p - \mathrm{Ad}(k)(\log p) \|)$$

for for $p \in \exp \mathfrak{p}_0$.

Assuming this for a moment, Lemma 7 can now be proved as follows. We have seen that $\mathrm{Ad}(a_0)$ never takes the eigenvalue 1 in $\mathfrak{m}_{\mathfrak{p}_0}$ and $\mathrm{Ad}(a_0) = \mathrm{Ad}(a_1)$ on $\mathfrak{m}_{\mathfrak{p}_0}$. Hence we can find a positive number c such that $\| X - \mathrm{Ad}(a_1)X \| \geqq c \| X \|$ for all $X \in \mathfrak{m}_{\mathfrak{p}_0}$. Therefore, from Lemma 8,

$$\| ma_1m^{-1} \| \geqq n^{\frac{1}{2}} \cosh(n^{-\frac{3}{2}}c \| \log m \|)$$

for all $m \in M_{\mathfrak{p}}$. But as we have seen above $\| ma_1m^{-1} \|$ remains bounded under the assumptions of Lemma 7, and so the same holds for $\| \log m \|$ and $\| m \|$.

Now in order to prove Lemma 8, we proceed as follows. Let E be the space of all endomorphisms of $\mathfrak{g}$. Put $\langle S, T\rangle = \mathrm{sp}(S^*T)$ $(S, T \in E)$, where S^* is the adjoint of S. This scalar product defines the structure of a Hilbert space on E. Let d_X $(X \in \mathfrak{g})$ denote the linear mapping of E given by $d_X T = [\mathrm{ad}\, X, T]$, where $[S, T] = ST - TS$ $(S, T \in E)$. If $X \in \mathfrak{p}_0$, $\mathrm{ad}\, X$ is self-adjoint, and therefore

$$\begin{aligned}\langle S, d_X T\rangle &= \mathrm{sp}(S^*[\mathrm{ad}\, X, T]) = -\mathrm{sp}([\mathrm{ad}\, X, S^*]T)\\ &= \mathrm{sp}((d_X S)^* T) = \langle d_X S, T\rangle.\end{aligned}$$

This proves that d_X is also self-adjoint. Moreover, if $p = \exp X \in \exp \mathfrak{p}_0$, it is obvious (by considering E as a Lie algebra under the bracket operation $[S, T]$) that $\exp d_X$ is the mapping σ_p: $T \to \mathrm{Ad}(p) T\, \mathrm{Ad}(p^{-1})$ $(T \in E)$ of E. Clearly σ_p is also self-adjoint. Hence we can choose an orthonormal base $(T_1, \cdots, T_r)$ of E consisting of eigen-vectors of d_X and σ_p. Let λ_i be the eigenvalue of d_X corresponding to T_i $(1 \leqq i \leqq r)$. Then if $T = \sum_{1 \leqq i \leqq r} c_i T_i$ $(c_i \in C)$, it is clear that $\sigma_p T = \sum_i c_i e^{\lambda_i} T_i$, and therefore $\| \sigma_p T \|^2 = \sum_i | c_i |^2 e^{2\lambda_i}$. Now put $T = \mathrm{Ad}(k)$, where k is some fixed element in K. Then this equation becomes

$$\| pkp^{-1} \|^2 = \sum_{1 \leqq i \leqq r} | c_i |^2 e^{2\lambda_i}.$$

On the other hand, since $\| Y \| = \| \theta(Y) \|$ $(Y \in \mathfrak{g})$, θ is a unitary transformation of $\mathfrak{g}$, and therefore $\| \theta S \theta^{-1} \| = \| S \|$ for any $S \in E$. Moreover, since $\theta(X) = -X$, it follows that $\theta(\mathrm{Ad}(pkp^{-1}))\theta^{-1} = \mathrm{Ad}(p^{-1}kp)$. Therefore

$$\begin{aligned}2 \| pkp^{-1} \|^2 &= \| pkp^{-1} \|^2 + \| p^{-1}kp \|^2 = \| \sigma_p T \|^2 + \| \sigma_{p^{-1}} T \|^2\\ &= 2 \sum_{1 \leqq i \leqq r} | c_i |^2 \cosh 2\lambda_i.\end{aligned}$$

But $\cosh 2t = 1 + 2 \sinh^2 t$ and $s(t) = \sinh t/t = \sum_{q \geqq 0} t^{2q}/(2q+1)!$ is an increasing function of t for $t \geqq 0$. Therefore

$$\| pkp^{-1} \|^2 = \sum_{1 \leqq i \leqq r} | c_i |^2 + 2 \sum_{1 \leqq i \leqq r} | c_i \lambda_i |^2 s(\lambda_i)^2.$$

Moreover, $\sum_i | c_i |^2 = \| k \|^2 = n$ since $\mathrm{Ad}(k)$ is unitary. Now choose an index j $(1 \leqq j \leqq r)$ such that $| c_j \lambda_j | = \max_{1 \leqq i \leqq r} | c_i \lambda_i |$. Since $| c_j | \leqq \| k \| = n^{\frac{1}{2}}$, it follows that $s(n^{-\frac{1}{2}} | c_j \lambda_j |) \leqq s(| \lambda_j |)$, and therefore

$$\begin{aligned}\| pkp^{-1} \|^2 &\geqq n + 2 | c_j \lambda_j |^2 s(\lambda_j)^2 \geqq n + 2 | c_j \lambda_j |^2 \{ s(n^{-\frac{1}{2}} | c_j \lambda_j |) \}^2\\ &= n \cosh(2n^{-\frac{1}{2}} | c_j \lambda_j |).\end{aligned}$$

On the other hand, $\| d_X T \|^2 = \sum_{1 \leqq i \leqq r} | c_i \lambda_i |^2 \leqq r \, | c_j \lambda_j |^2$ and $r = \dim E = n^2$. Therefore $| c_j \lambda_j | \geqq n^{-1} \| d_X T \|$ and

$$\| pkp^{-1} \| \geqq n^{\frac{1}{2}} \cosh (n^{-\frac{3}{2}} \| d_X T \|)$$

since $\cosh t$ is an increasing function of t for $t \geqq 0$ and $\cosh 2t \geqq \cosh^2 t$. But $T = \mathrm{Ad}(k)$ is unitary, and therefore

$$\begin{aligned} \| d_X T \| &= \| (d_X T) T^{-1} \| = \| (\mathrm{ad}\, X) - T (\mathrm{ad}\, X) T^{-1} \| \\ &= \| \mathrm{ad} (X - \mathrm{Ad}(k) X) \| = \| X - \mathrm{Ad}(k) X \|. \end{aligned}$$

This proves that

$$\| pkp^{-1} \| \geqq n^{\frac{1}{2}} \cosh (n^{-\frac{3}{2}} \| X - \mathrm{Ad}(k) X \|)$$

which is equivalent to the statement of Lemma 8.

The second result which was required during the proof of Lemma 6, may be stated as follows.

LEMMA 9. *Suppose* n *varies in* N'' *in such a way that* $\| a_0^{-1} n a_0 n^{-1} \|$ *remains bounded. Then* $\| n \|$ *itself remains bounded.*

Consider the base $(X_1, \cdots, X_q)$ of $\mathfrak{n}$ introduced during the proof of Lemma 6 and let $(t_1, \cdots, t_q)$ denote the complex Cartesian coordinates in $\mathfrak{n}$ corresponding to this base. For any j $(1 \leqq j \leqq q)$, define the projection π_j as in Lemma 2, and put $\pi_0 = 0$ and $\mathfrak{n}_j = \pi_j \mathfrak{n}$ $(0 \leqq j \leqq q)$. Then from Lemma 2, there exist polynomial functions p_j on $\mathfrak{n}_{j-1} \times \mathfrak{n}_{j-1}$ such that

$$t_j (\log (\exp Y_1 \exp Y_2)) = t_j (Y_1 + Y_2) + p_j (\pi_{j-1} Y_1, \pi_{j-1} Y_2) \quad (1 \leqq j \leqq q)$$

for $Y_1, Y_2 \in \mathfrak{n}$. Now put $X = \log n$. Then it would be enough to prove that $t_j(X)$ $(1 \leqq j \leqq q)$ all remain bounded. Suppose this is false. Then consider the least index j such that $| t_j(X) |$ does not stay bounded. Put

$$Z = \log (a_0^{-1} n a_0 n^{-1}) = \log (\exp (\mathrm{Ad} (a_0^{-1}) X) \exp (-X)).$$

Then

$$t_j(Z) = t_j (\mathrm{Ad} (a_0^{-1}) X) - t_j (X) + p_j (\pi_{j-1} \mathrm{Ad} (a_0^{-1}) X, -\pi_{j-1} X).$$

But since X_i is an eigenvector of $\mathrm{Ad}(a_0)$, $\mathrm{Ad}(a_0) X_i = c_i X_i$ $(1 \leqq i \leqq q)$, where c_i are nonzero complex numbers. Therefore $t_i (\mathrm{Ad} (a_0^{-1}) X) = c_i^{-1} t_i (X)$ and

$$(c_j^{-1} - 1) t_j (X) = t_j (Z) - p_j (\pi_{j-1} \mathrm{Ad} (a_0^{-1}) X, -\pi_{j-1} X).$$

In view of the hypothesis of the lemma and our choice of j, the right side remains bounded as n varies. Moreover, $c_j \neq 1$ if $X_j \in \mathfrak{n}''$, and $t_j(X) = 0$ if $X_j \in \mathfrak{n}'$. Therefore, it follows from the above equation that $t_j(X)$ remains bounded in either case. As this contradicts the definition of j, the lemma is proved.

The proof of Theorem 1 is now quite complete.

3. The sets V and V_C. In order to prove our next result, we need a simple lemma. Let W be a vector space over C of finite dimension. We shall call an endomorphism X of W unipotent if $X-1$ is nilpotent. (Here 1 stands for the identity mapping of W.)

LEMMA 10. *Let $\mathfrak{N}$ and $\mathcal{E}$, respectively, be the sets of all nilpotent and unipotent endomorphisms of W. Then $X \to \exp X$ $(X \in \mathfrak{N})$ is a one-one mapping of $\mathfrak{N}$ onto $\mathcal{E}$.*

Since $\exp X - 1 = \sum_{k \geqq 1} X^k/k!$, it is obvious that $\exp X \in \mathcal{E}$ for $X \in \mathfrak{N}$. For any $Y \in \mathcal{E}$, define $\log Y = \sum_{k \geqq 1} (-1)^{k-1}(Y-1)^k/k$. Since Y is unipotent, this series is actually finite, and it is clear that $\log Y \in \mathfrak{N}$. Our assertion now follows from the well-known identities (see Birkhoff [1]) $X = \log(\exp X)$ $(X \in \mathfrak{N})$ and $Y = \exp(\log Y)$ $(Y \in \mathcal{E})$.

Now G being as in Theorem 1, we shall prove the following result.

LEMMA 11. *Let V be the open set in the real Euclidean space $\mathfrak{g}_0$ defined as follows. An element X of $\mathfrak{g}_0$ lies in V if and only if the absolute value of every eigenvalue of $\operatorname{ad} X$ is less than[7] π. Then the exponential mapping of $\mathfrak{g}_0$ into G is regular and univalent on V.*

If $X \in V$, it is clear that $\operatorname{ad} X$ can never have an eigenvalue of the form $2\pi(-1)^{\frac{1}{2}}n$ where n is a nonzero integer. Therefore

$$(1-\exp(-\operatorname{ad} X))/\operatorname{ad} X = \sum_{m \geqq 0} (-1)^m (\operatorname{ad} X)^m/(m+1)!$$

is a nonsingular transformation of $\mathfrak{g}_0$. This shows (see Chevalley [2(a), p. 157]) that the exponential mapping is regular at X. Now suppose $\exp X_1 = \exp X_2$ $(X_1, X_2 \in V)$. Put $\sigma = (1-\exp(-\operatorname{ad} X_1))/\operatorname{ad} X_1$. Then $\operatorname{Ad}(x) - 1 = \exp(\operatorname{ad} X_1) - 1 = \operatorname{Ad}(x)\sigma \operatorname{ad} X_1$, where $x = \exp X_1 = \exp X_2$. Since $\operatorname{Ad}(x)$ and σ are both nonsingular, it follows that $\operatorname{Ad}(x)Y = Y$ for some $Y \in \mathfrak{g}$ if and only if $(\operatorname{ad} X_1)Y = 0$. Let $\mathfrak{c}_0$ denote the centralizer of x in $\mathfrak{g}_0$. Then $\mathfrak{c}_0$ is also the centralizer of X_1 in $\mathfrak{g}_0$. But obviously $\operatorname{Ad}(x)X_2 = X_2$, and therefore X_1, X_2 commute. Hence $\exp(X_1 - X_2) = \exp X_1 \exp(-X_2) = 1$. Let λ_{ji} $(1 \leqq j \leqq r_i)$ denote all the distinct eigenvalues of $\operatorname{ad} X_i$ $(i = 1, 2)$. Then every eigenvalue of $\operatorname{ad}(X_1 - X_2)$ must be of the form $\lambda_{j1}-\lambda_{k2}$ for some j and k. Moreover it follows from the definition of V that $|\lambda_{j1}-\lambda_{k2}|<2\pi$. Hence $\exp(\lambda_{j1}-\lambda_{k2})\neq 1$ unless $\lambda_{j1}=\lambda_{k2}$. Therefore since $\exp\operatorname{ad}(X_1-X_2)=\operatorname{Ad}(\exp(X_1-X_2))=1$, zero is the only eigenvalue of $\operatorname{ad}(X_1-X_2)$. This implies that $\operatorname{ad}(X_1-X_2)$ is nilpotent, and so it follows from Lemma 10 that $\operatorname{ad}(X_1-X_2)=0$. But $\mathfrak{g}$ being semisimple, we can now conclude that $X_1=X_2$, and therefore the exponential mapping is univalent on V.

---

[7] Here π denotes, as usual, the smallest positive root of the equation $\sin t = 0$.

Let V_G denote the image of V in G under the exponential mapping and let Z denote the center of G. Obviously V_G is open in G.

COROLLARY. *If $z\in Z$ then V_G does not intersect zV_G unless $z=1$.*

This follows by applying Lemma 11 to G/Z instead of G.

The following property of V is important for our applications.

LEMMA 12. *Let X_r $(r\geqq 1)$ be a sequence in V. Then if $\|\exp X_r\|$ remains bounded, the same holds for $\|X_r\|$.*

For the purpose of this lemma we can obviously replace G by any connected group locally isomorphic to it. Hence we may assume that $G\subset G_c$ (see § 2). We shall now use the notation of the proofs of Lemmas 3 and 4. Put $\mathfrak{g}_1=\bigcup_{u\in U}\operatorname{Ad}(u)(\mathfrak{h}+\mathfrak{n})$. Since $G=UA_cN_c$ and $\mathfrak{h}+\mathfrak{n}$ is invariant under $\operatorname{Ad}(A_cN_c)$, it is obvious that $\operatorname{Ad}(x)\mathfrak{g}_1=\mathfrak{g}_1$ for $x\in G_c$. Since every regular element of $\mathfrak{g}$ is conjugate to some element in $\mathfrak{h}$ under G_c (see Chevalley [2(b)]), $\mathfrak{g}_1$ contains the set of all regular elements in $\mathfrak{g}$. On the other hand, since U is compact it is clear that $\mathfrak{g}_1$ is closed in $\mathfrak{g}$. Therefore, since regular elements are dense in $\mathfrak{g}$, $\mathfrak{g}=\mathfrak{g}_1$. Hence we can choose $u_r\in U$ and $Y_r\in\mathfrak{h}+\mathfrak{n}$ such that $X_r=\operatorname{Ad}(u_r)Y_r$. Since $\operatorname{Ad}(u_r)$ is unitary, $\|X_r\|=\|Y_r\|$ and $\|\exp X_r\|=\|\exp Y_r\|$. Let $Y_r=H_r+Z_r$ $(H_r\in\mathfrak{h}, Z_r\in\mathfrak{n})$. One proves without difficulty that the eigenvalues of $\operatorname{ad}Y_r$ and $\operatorname{ad}H_r$ are the same. Therefore since $X_r\in V$, it follows that $|\alpha(H_r)|<\pi$ for every root $\alpha\in P$. This shows that $\|H_r\|$ remains bounded. Now let $F(t)$ denote the entire function on the complex plane given by the series

$$F(t)=\sum_{m\geqq 0}(-1)^m t^m/(m+1)!=(1-e^{-t})/t.$$

Let H_0 be a fixed element in $\mathfrak{h}$ and let t_α $(\alpha\in P)$ denote the complex Cartesian coordinates in $\mathfrak{n}$ corresponding to the base X_α $(\alpha\in P)$. Then if $H\in\mathfrak{h}$ and $Z\in\mathfrak{n}$, it is obvious that $\operatorname{Ad}(\exp(H+Z))H_0-H_0\in\mathfrak{n}$. For any $\beta\in P$, consider the function

$$f_\beta(H,Z)=t_\beta(\operatorname{Ad}(\exp(H+Z))H_0-H_0)+e^{\beta(H)}F(\beta(H))\beta(H_0)t_\beta(Z)$$

on $\mathfrak{h}+\mathfrak{n}$ $(H\in\mathfrak{h}, Z\in\mathfrak{n})$. Obviously, it is holomorphic. Moreover, if $\beta<\gamma$ $(\gamma\in P)$, it is easily seen that $f_\beta(H,Z+tX_\gamma)=f_\beta(H,Z)$ $(t\in C)$. Hence f_β depends only on H and $t_\alpha(Z)$ $(0<\alpha\leqq\beta)$. Let us now consider $\{(d/dt)f_\beta(H,Z+tX_\beta)\}_{t=0}$. We know (see Chevalley [2(a), p. 157]) that

$$\{(d/dt)\operatorname{Ad}(\exp(H+Z+tX_\beta))H_0\}_{t=0}=\operatorname{Ad}(\exp(H+Z))(\operatorname{ad}Y)H_0,$$

where

$$Y=\{(1-\exp(-\operatorname{ad}(H+Z)))/\operatorname{ad}(H+Z)\}X_\beta$$
$$\equiv F(\beta(H))X_\beta \mod \sum_{\gamma>\beta} CX_\gamma.$$

Therefore

$$\{(d/dt)f_\beta(H,Z+tX_\beta)\}_{t=0}=F(\beta(H))t_\beta(\operatorname{Ad}(\exp(H+Z))[X_\beta,H_0])$$
$$+e^{\beta(H)}F(\beta(H))\beta(H_0).$$

But $[X_\beta,H_0]=-\beta(H_0)X_\beta$ and $\operatorname{Ad}(\exp(H+Z))X_\beta\equiv e^{\beta(H)}X_\beta \mod \sum_{\gamma>\beta} CX_\gamma$. Hence, it follows that $\{(d/dt)f_\beta(H+Z+tX_\beta)\}_{t=0}=0$, and therefore f_β depends only on H and $t_\alpha(Z)$ $(0<\alpha<\beta)$.

Now suppose the assertion of the lemma is false. Then there exists a root $\beta\in P$ such that $t_\beta(Z_r)$ does not remain bounded. Select the least such root β. Then $\|H_r\|$ and $t_\alpha(Z_r)$ $(0<\alpha<\beta)$ all remain bounded and therefore $f_\beta(H_r,Z_r)$ also remains bounded as $r\to\infty$. On the other hand, by our hypothesis, $\|\exp Y_r\|$, and therefore, also, $\|\operatorname{Ad}(\exp(H_r+Z_r))\|$ stay bounded. Hence the same holds for

$$e^{\beta(H_r)}F(\beta(H_r))\beta(H_0)t_\beta(Z_r)=f_\beta(H_r,Z_r)-t_\beta(\operatorname{Ad}(\exp(H_r+Z_r))H_0-H_0).$$

On the other hand, $|\beta(H_r)|<\pi$, and so $e^{-\beta(H_r)}\{F(\beta(H_r))\}^{-1}$ also remains bounded. Therefore by choosing H_0 in such a way that $\beta(H_0)\neq 0$, we conclude that $t_\beta(Z_r)$ also remains bounded. As this contradicts the definition of β, the lemma follows.

Let us say that a sequence x_r $(r\geqq 1)$ in G tends to infinity, if for every compact set ω of G, we can select a positive integer r_0 such that $x_r\notin\omega$ for $r\geqq r_0$. Obviously if $x_r\to\infty$, the same holds for any subsequence of $\{x_r\}$.

COROLLARY. *Let z_r $(r\geqq 1)$ be a sequence in Z which tends to infinity. Then if $x_r\in z_rV_G$, x_r also tends to infinity.*

For otherwise, by selecting a subsequence, we can arrange that x_r converges to some $x\in G$. But $x_r=z_r\exp X_r$, where $X_r\in V$ and $\|x_r\|=\|\exp X_r\|$ remains bounded. Therefore by Lemma 12, $\|X_r\|$ also remains bounded and so again by selecting a subsequence, we may suppose that X_r converges to some $X \in \mathfrak{g}_0$. Then $z_r = x_r \exp(-X_r) \to x \exp(-X)$, contradicting our hypothesis that $z_r \to \infty$.

Part II.

4. Proof of Theorem 2. Let A be a Cartan subgroup of G (see [4(c), § 2]) and $\mathfrak{h}_0$ the Lie algebra of A. We assume that $\theta(\mathfrak{h}_0) = \mathfrak{h}_0$. Let $x \to x^*$ $(x \in G)$ denote the natural mapping of G on $G^* = G/A$ and put $h^{x^*} = xhx^{-1}$ $(x \in G, h \in A)$. We shall call a subset of G bounded if its closure is compact.

LEMMA 13. *Let ω be a bounded set in G and B the set of all $h \in A$ such that $h^{x^*} \in \omega$ for some $x^* \in G^*$. Then B is also bounded.*

Let h_r $(r \geqq 1)$ be a sequence of points in B. We have to show that some subsequence of $\{h_r\}$ is convergent. Choose $x_r \in G$ such that $h_r^{x_r^*} \in \omega$, and for any $y \in G$, define $\lambda(y)$ as follows. If $\lambda_1, \cdots, \lambda_s$ are all the distinct eigenvalues of $\mathrm{Ad}(y)$ and m_i is the multiplicity of λ_i, then

$$\lambda(y) = m_1 |\lambda_1|^2 + \cdots + m_s |\lambda_s|^2.$$

Since ω is bounded, we can find a positive number M such that $\lambda(y) \leqq M$ for all $y \in \omega$. Hence $\lambda(h_r) = \lambda(h_r^{x_r^*}) \leqq M$. But it is obvious that $\lambda(h) = \| h \|^2$ for $h \in A$ (in the notation of § 2). Therefore $\| h_r \|^2 \leqq M$, and so by selecting a subsequence, we can arrange that $\mathrm{Ad}(h_r)$ is convergent. Choose $h_\infty \in A$ such that $\mathrm{Ad}(h_r) \to \mathrm{Ad}(h_\infty)$. Then $\mathrm{Ad}(h_r'') \to 1$ if $h_r'' = h_r h_\infty^{-1}$, and Z being the center of G, it is obvious that we can select $z_r \in Z$ such that $h_r' = z_r^{-1} h_r''$ converges to 1 in G. Since $h_r = z_r h_r' h_\infty$, it is enough to show that some subsequence of z_r is convergent or, what is equivalent, that z_r cannot tend to infinity. Let Ξ_∞ denote the centralizer of h_∞ in G and $\bar{x}_r$ the coset $x_r \Xi_\infty$ in G/Ξ_∞. Since $\mathrm{Ad}(h_r) \to \mathrm{Ad}(h_\infty)$ and $h_r^{x_r^*} \in \omega$, we can. by applying Theorem 1 to $\mathrm{Ad}(G) \cong G/Z$ at the point $\mathrm{Ad}(h_\infty)$, conclude that $\bar{x}_r$ are all contained in a compact subset of G/Ξ_∞. But $z_r(h_r')^{x_r^*} = (h_r h_\infty^{-1})^{x_r^*}$. Therefore, since $h_r^{x_r^*} \in \omega$, the right side remains within a compact subset of G. Moreover $h_r' \to 1$, and so we can assume without loss of generality that $h_r' \in V_G$ (in the notation of § 3). Then $(h_r')^{x_r^*}$ is also in V_G, and hence it follows from the Corollary of Lemma 12 that z_r cannot tend to infinity. This proves the lemma.

From now on let us agree to use the notation of [4(h), § 5]. For any $\alpha \in P$, let η_α denote the character of A given by $\mathrm{Ad}(h)X_\alpha = \eta_\alpha(h)X_\alpha$ $(h \in A)$. Put

$$\Delta'(h) = \prod_{\alpha \in P} (1 - \eta_\alpha(h^{-1})) \qquad (h \in A).$$

Let A' be the set of those points $h \in A$ where $\Delta'(h) \neq 0$. Then A' is exactly the set of regular elements in A (see [4(c), § 2]). Let dx^* denote the invariant measure on $G^* = G/A$.

LEMMA 14. Put[1]

$$F_f(h) = \Delta'(h) \int_{G^*} f(h^{x^*})\, dx^* \qquad (h \in A', f \in C_c^\infty(G)).$$

Then the above integral is convergent and F_f is a function of class C^∞ on A'.

Fix $f \in C_c^\infty(G)$ and $h_0 \in A'$, and select a compact set ω in G such that f is zero outside ω. Then if Ξ is the centralizer of h_0 in G, it follows from the Corollary of Lemma 3 of [4(c)] that Ξ/A is finite. Hence by Theorem 1, we can select an open neighborhood B of h_0 in A' and a compact set Ω^* in G^* with the following property. If $xhx^{-1} \in \omega$ for some $h \in B$ and $x \in G$, then $x^* \in \Omega^*$. Therefore it is clear that

$$\int_{G^*} f(h^{x^*})\, dx^* = \int_{\Omega^*} f(h^{x^*})\, dx^* \qquad (h \in B),$$

and from this our lemma follows immediately.

Let $\mathfrak{B}$ be the universal enveloping algebra of $\mathfrak{g}$ and $\mathfrak{H}$ the subalgebra of $\mathfrak{B}$ generated by $(1, \mathfrak{h})$. Then we can regard the elements of $\mathfrak{B}$ and $\mathfrak{H}$ as left-invariant differential operators on G and A, respectively (see [4(c), § 4]). $S(\mathfrak{h})$ being the symmetric algebra over $\mathfrak{h}$, there exists a unique isomorphism of $S(\mathfrak{h})$ onto $\mathfrak{H}$ which preserves 1 and also every element in $\mathfrak{h}$. For any $q \in S(\mathfrak{h})$, we denote by $\partial(q)$ the image of q under this isomorphism. Then $\partial(q)$ is a differential operator on A.

Let A_1 be an open subset of A. We regard it as an open submanifold of A and consider the space $\mathcal{C}_0(A_1)$ of all complex-valued functions g on A_1 of class C^∞ satisfying the following two conditions.

(1) g vanishes (on A_1) outside some bounded subset of A_1.

(2) For every[1] $v \in \mathfrak{H}$,

$$\tau_v(g) = \sup_{h \in A_1} |g(h; v)| < \infty.$$

Define a topology in $\mathcal{C}_0(A_1)$ by means of the collection of seminorms τ_v ($v \in \mathfrak{H}$). Then $\mathcal{C}_0(A_1)$ is a locally convex space and the same holds for $C_c^\infty(G)$ under its usual topology (see Schwartz [6, p. 67]). Our main object now is to prove the following theorem.

THEOREM 2. *Let*

$$F_f(h) = \Delta'(h) \int_{G^*} f(h^{x^*})\, dx^* \qquad (h \in A', f \in C_c^\infty(G)).$$

Then $F_f \in \mathscr{B}_0(A')$, *and* $f \to F_f$ *is a continuous mapping of* $C_c^\infty(G)$ *into* $\mathscr{B}_0(A')$. *Moreover, for any bounded open subset* ω *of* G, *we can select a bounded subset* B *of* A' *such that* F_f *is zero outside* B *for every*[1] $f \in C_c^\infty(\omega)$.

We begin by first proving the following weaker result.

LEMMA 15. *There exists an open neighborhood* ${}_0A$ *of* 1 *in* A *with the following property. Put* ${}_0A' = {}_0A \cap A'$ *and let* ${}_0F_f$ *denote the restriction of* F_f *on* ${}_0A'$ $(f \in C_c^\infty(G))$. *Then* ${}_0F_f \in \mathscr{B}_0({}_0A')$, *and* $f \to {}_0F_f$ *is a continuous mapping of* $C_c^\infty(G)$ *into* $\mathscr{B}_0({}_0A')$.

Let l be the rank of $\mathfrak{g}$ and n the complex dimension of $\mathfrak{g}$. Then if λ is an indeterminate and I the identity mapping of $\mathfrak{g}$,

$$\det(\lambda I - \operatorname{ad} X) = \lambda^n + \sum_{l \leqq r < n} (-1)^r p_r(X) \lambda^r \qquad (X \in \mathfrak{g}),$$

where[8] $p_r \in I(\mathfrak{g})$. Then if ϵ is a sufficiently small positive number, the inequalities $|p_r(X)| \leqq \epsilon$ $(l \leqq r < n)$ imply that every eigenvalue of $\operatorname{ad} X$ is less that $\pi/2$ in absolute value. Choose a function $\phi(t)$ of class C^∞ of $(n-l)$ real variables t_r $(l \leqq r < n)$ such that $\phi(t) = 0$ unless $\max_r |t_r| \leqq \epsilon$ and $\phi(t) = 1$ if $\max_r |t_r| \leqq \epsilon/2$. Let $\Phi(X)$ denote the function on $\mathfrak{g}_0$ obtained from ϕ under the substitution $t_r = p_r(X)$ $(X \in \mathfrak{g}_0)$. Define V as in § 3 and let V_0 be the set of those $X \in V$ where $\max_r |p_r(X)| < \epsilon/3$. Then obviously, V_0 is an open neighborhood of zero in V and $\operatorname{Ad}(x)V_0 = V_0$, $(x \in G)$. For a given $f \in C_c^\infty(G)$, consider the function $\bar{f}$ on $\mathfrak{g}_0$ defined by $\bar{f}(X) = f(\exp X)\Phi(X)$ $(X \in \mathfrak{g}_0)$. It is obvious that the carrier of $\bar{f}$ is contained in V and $\bar{f}(X) = f(\exp X)$ for $(X \in V_0)$. Now define $x^*H = \operatorname{Ad}(x)H$ $(x \in G, H \in \mathfrak{h})$ and $\pi = \prod_{\alpha \in P} \alpha$. Let $\mathfrak{h}_0'$ be the set of those points $H \in \mathfrak{h}_0$ where $\pi(H) \neq 0$. The function $(1 - e^{-z})/z$ of the complex variable z, is holomorphic at $z = 0$ and takes the value 1 there. Therefore, since $\eta_\alpha(\exp H) = e^{\alpha(H)}$ $(H \in \mathfrak{h}_0)$, it is clear that we can select an open neighborhood $\mathfrak{h}_2$ of zero in $\mathfrak{h}_0 \cap V_0$ and an analytic function ζ on $\mathfrak{h}_2$ such that

$$\Delta'(\exp H) = \zeta(H)\pi(H) \qquad (H \in \mathfrak{h}_2).$$

Choose another open neighborhood $\mathfrak{h}_1$ of zero in $\mathfrak{h}_0$ such that the closure of $\mathfrak{h}_1$ is compact and contained in $\mathfrak{h}_2$. Obviously, $\zeta(0) = 1$ and ζ is never zero on $\mathfrak{h}_2$. Put $\mathfrak{h}_1' = \mathfrak{h}_1 \cap \mathfrak{h}_0'$ and ${}_0A = \exp \mathfrak{h}_1$. Then ${}_0A$ is an open neighborhood of 1 in A and $\exp H \in {}_0A' = {}_0A \cap A'$ if $H \in \mathfrak{h}_1'$. For any $g \in C_c^\infty(\mathfrak{g}_0)$, put

---

[8] We are using here the notation of [4(g)].

$$\phi_g(H) = \pi(H) \int_{G^*} g(x^*H)\, dx^* \qquad (H \in \mathfrak{h}_1').$$

It follows from Theorem 3 of [4(h)] that the above integral is convergent and[8] $\phi_g \in \mathscr{C}(\mathfrak{h}_1')$. Moreover, it is obvious that $F_f(\exp H) = \zeta(H)\phi_{\bar{f}}(H)$ $(H \in \mathfrak{h}_1')$. But it follows from the definition of $\mathfrak{h}_1$, that[9] $\partial(q)\zeta$ remains bounded on $\mathfrak{h}_1$ for every $q \in S(\mathfrak{h})$. Therefore $\phi \rightarrow \zeta\phi$ $(\phi \in \mathscr{C}(\mathfrak{h}_1'))$ is a continuous mapping of $\mathscr{C}(\mathfrak{h}_1')$ into itself. In view of Theorem 3 of [4(h)], this proves that $g \rightarrow \zeta\phi_g$ $(g \in C_c^\infty(\mathfrak{g}_0))$ is a continuous mapping of $C_c^\infty(\mathfrak{g}_0)$ into $\mathscr{C}(\mathfrak{h}_1')$. On the other hand, ${}_0A' = \exp \mathfrak{h}_1'$ and, since the exponential mapping is one-one and regular on $\mathfrak{h}_2$ and the closure of $\mathfrak{h}_1$ is compact, it is clear that a function ψ on ${}_0A'$ lies in $\mathscr{C}_0({}_0A')$ if and only if the function $\psi'(H) = \psi(\exp H)$ $(H \in \mathfrak{h}_1')$ lies in $\mathscr{C}(\mathfrak{h}_1')$. Moreover, it is obvious that $\psi \rightarrow \psi'$ is a topological mapping of $\mathscr{C}_0({}_0A')$ onto $\mathscr{C}(\mathfrak{h}_1')$. Put $F_f'(H) = F_f(\exp H)$ $(f \in C_c^\infty(G), H \in \mathfrak{h}_1')$. Then it would be enough to show that $F_f' \in \mathscr{C}(\mathfrak{h}_1')$ and $f \rightarrow F_f'$ is a continuous mapping of $C_c^\infty(G)$ into $\mathscr{C}(\mathfrak{h}_1')$. But we have just seen that $F_f' = \zeta\phi_{\bar{f}}$, and therefore, in view of what has been said above, it is sufficient to prove that $\sigma: f \rightarrow \bar{f}$ is a continuous mapping of $C_c^\infty(G)$ into $C_c^\infty(\mathfrak{g}_0)$. Let ω be a bounded open subset of G. Since $C_c^\infty(\mathfrak{g}_0)$ is a locally convex space, it would be enough to prove that σ is continuous on $C_c^\infty(\omega)$ (see Schwartz [6, p. 69, Theorem II]). Let $\bar{\omega}$ denote the closure of ω and W the carrier of Φ. Then $W \subset V$, and it follows from Lemma 12 that $\exp W$ is closed in G. Hence $\bar{\omega} \cap \exp W$ is compact. Let Ω denote the complete inverse image of $\bar{\omega} \cap \exp W$ in V under the exponential mapping. Then by Lemma 11, Ω is also compact. Select an open neighborhood Ω_1 of Ω in $\mathfrak{g}_0$ such that its closure $\bar{\Omega}_1$ is compact and contained in V. Then for any $p \in S(\mathfrak{g})$, $\partial(p)\Phi$ remains bounded on Ω_1. Since the exponential mapping defines an analytic isomorphism of V with V_G, it is now clear that for any $q \in S(\mathfrak{g})$, we can choose a finite number of elements $b_1, \cdots, b_m \in \mathfrak{B}$ such that

$$|\bar{f}(X; \partial(q))| \leqq \sum_{1 \leqq i \leqq m} |f(\exp X; b_i)|$$

for all $f \in C_c^\infty(\omega)$ and $X \in \Omega_1$. But since $\bar{f}$ is zero (on $\mathfrak{g}_0$) outside Ω, this obviously implies that σ is continuous on $C_c^\infty(\omega)$. Hence the lemma is proved.

Now fix a point h_0 in A and let Ξ and $\mathfrak{z}_0$ be the centralizers of h_0 in G

---

[8] We are using here the notation of [4(h), § 5].

and $\mathfrak{g}_0$, respectively. Then as we have already seen in § 2, $\mathfrak{z}_0$ is reductive in $\mathfrak{g}_0$ and $\operatorname{rank}\mathfrak{z}_0 = \operatorname{rank}\mathfrak{g}_0$. Let Ξ_0 be the analytic subgroup of G corresponding to $\mathfrak{z}_0$. Then we know from Lemma 15 of [4(i)] that $\Xi/\Xi_0 Z$ is finite. Put $\bar{G} = G/\Xi$ and let $x \rightarrow \bar{x}$ $(x \in G)$ denote the natural mapping G on $\bar{G}$. Since $\mathfrak{z}_0$ is reductive, there exists (see Weil [7, p. 45]) an invariant measure $d\bar{x}$ on $\bar{G}$. Similarly there exists a measure $d\xi^*$ on $\Xi^* = \Xi/A$ which is invariant under the operations of Ξ. It is well known (see Weil [7]) that $d\bar{x}$ and $d\xi^*$ can be normalized that[1]

$$\int \gamma(x^*)\,dx^* = \int \bar{\gamma}(\bar{x})\,d\bar{x} \qquad (\gamma \in C_c(G^*)),$$

where

$$\bar{\gamma}(\bar{x}) = \int_{\Xi^*} \gamma(x\xi^*)\,d\xi^* \qquad (x \in G)$$

and $xy^* = (xy)^*$ $(x, y \in G)$. Select an open, connected and bounded neighborhood B_0 of 1 in A_0 such that $B = h_0 B_0$ satisfies the condition of Theorem 1. We assume that B_0 is so small that $|\eta_\alpha(h) - 1| \geqq \frac{1}{2}|\eta_\alpha(h_0) - 1|$ for $h \in B$ and $\alpha \in P$. Let $\mathfrak{z}$ be the complexification of $\mathfrak{z}_0$ in $\mathfrak{g}$ and P_1 the set of all roots $\alpha \in P$ for which $X_\alpha \in \mathfrak{z}$. Also let P_2 the the complement of P_1 in P. Then if

$$\Delta_i' = \prod_{\alpha \in P_i} (1 - \eta_\alpha^{-1}) \qquad (i = 1, 2),$$

it is clear that Δ_2' is never zero on B and $\Delta'(h_0 h) = \Delta_1'(h)\Delta_2'(h_0 h)$ $(h \in B_0)$. Hence $B_0' = h_0^{-1}(B \cap A')$ consists of all those $h \in B_0$ where $\Delta_1'(h) \neq 0$. Let Ξ_0^* denote the image of Ξ_0 in Ξ^* and put $\Xi_1 = \Xi_0 A$. Since Ξ_0 is normal in Ξ, Ξ_1 is a group and $\Xi_1 \supset \Xi_0 Z$. Therefore, in view of the finiteness of $\Xi/\Xi_0 Z$, we can select a finite number of elements $y_1 = 1, y_2, \cdots, y_r$ in Ξ such that Ξ is the disjoint union of the cosets $y_i \Xi_1$ $(1 \leqq i \leqq r)$. Then Ξ^* is the disjoint union of the open sets $y_i \Xi_0^*$ $(1 \leqq i \leqq r)$ and $\Xi_0^* \cong \Xi_0/\Xi_0 \cap A$. Since $\mathfrak{z}_0$ is reductive, Lemma 15 is obviously applicable to Ξ_0 in place of G. Moreover, $B_0 \subset \Xi_0$ since B_0 is connected. Put

$$\psi_g(h) = \Delta_1'(h) \int_{\Xi_0^*} g(h^{\xi^*})\,d\xi^* \qquad (h \in B_0')$$

for $g \in C_c^\infty(\Xi_0)$. Then if B_0 is chosen sufficiently small, it follows from Lemma 15 (applied to Ξ_0) that $\psi_g \in \mathcal{B}_0(B_0')$ and $g \rightarrow \psi_g$ is a continuous mapping of $C_c^\infty(\Xi_0)$ into $\mathcal{B}_0(B_0')$.

Now if $f \in C_c^\infty(G)$, it is clear that

$$\int_{G^*} f(h^{x^*})\,dx^* = \int_{\bar{G}} f(h : \bar{x})\,d\bar{x} \qquad (h \in B \cap A'),$$

where

$$f(h:\bar{x}) = \int_{\Xi^*} f(xh^{\xi^*}x^{-1})\,d\xi^* = \sum_{1\leqq i\leqq r} \int_{\Xi_0^*} f(xy_ih^{\xi^*}y_i^{-1}x^{-1})\,d\xi^* \qquad (x \in G).$$

Let ω be a bounded open subset of G. Then it follows from our definition of B that there exists a compact set $\bar{\Omega}$ in $\bar{G}$ with the following property. If $xhx^{-1} \in \omega$ for some $x \in G$ and $h \in B$, then $\bar{x} \in \bar{\Omega}$. Let dx and $d\xi$ denote the Haar measures on G and Ξ, respectively. We normalize them in such a way that

$$\int_G \gamma(x)\,dx = \int_{\bar{G}} \gamma'(\bar{x})\,d\bar{x} \qquad (\gamma \in C_c(G))$$

where $\gamma'(\bar{x}) = \int \gamma(x\xi)\,d\xi$ $(x \in G)$. Select a function $\alpha \in C_c(G)$ such that $\alpha' = 1$ on $\bar{\Omega}$ and put

$$g_f(\xi) = \sum_{1\leqq i\leqq r} \int_G \alpha(x) f(xy_ih_0\xi y_i^{-1}x^{-1})\,dx \qquad (\xi \in \Xi_0)$$

for any $f \in C_c^\infty(\omega)$. Then it is clear that

$$\int_{G^*} f((h_0h)^{x^*})\,dx^* = \int_{\bar{\Omega}} f(h_0h:\bar{x})\,d\bar{x} = \int_{\Xi_0^*} g_f(h^{\xi^*})\,d\xi^* \qquad (h \in B_0')$$

for $f \in C_c^\infty(\omega)$. Put

$$\beta'(h) = \Delta_2'(h)\beta(h_0^{-1}h) \qquad (h \in B \cap A')$$

for $\beta \in \mathscr{B}_0(B_0')$. It is obvious that Δ_2' is bounded away from zero on B. Therefore $\beta \rightarrow \beta'$ is a continuous mapping of $\mathscr{B}_0(B_0')$ onto $\mathscr{B}(B \cap A')$. On the other hand, if $f \in C_c^\infty(\omega)$,

$$\begin{aligned} F_f(h_0h) &= \Delta'(h_0h) \int_{G^*} f((h_0h)^{x^*})\,dx^* \\ &= \Delta_2'(h_0h)\psi_{g_f}(h) \qquad (h \in B_0'), \end{aligned}$$

and therefore $F_f = \psi_{g_f}'$ on $B \cap A'$. The mapping $f \rightarrow g_f$ of $C_c^\infty(\omega)$ into $C_c^\infty(\Xi_0)$ is obviously continuous. Therefore $f \rightarrow \psi_{g_f}'$ is a continuous mapping of $C_c^\infty(\omega)$ into $\mathscr{B}_0(B \cap A')$. Thus we have obtained the following improved version of Lemma 15.

LEMMA 16. *Let h_0 be a point in A. Then there exists an open neighborhood ${}_0A$ of h_0 in A with the following property. Put ${}_0A' = {}_0A \cap A'$ and let ${}_0F_f$ denote the restriction of F_f on ${}_0A'$ $(f \in C_c^\infty(G))$. Then ${}_0F_f \in \mathscr{B}_0({}_0A')$ and $f \rightarrow {}_0F_f$ is a continuous mapping of $C_c^\infty(G)$ into $\mathscr{B}_0({}_0A')$.*

It is now easy to deduce Theorem 2. Let ω be a nonempty bounded open set in G. Define B as in Lemma 13. Then it follows from Lemma 16 and the boundedness of B that there exist a finite number of nonempty open subsets A_i of A $(1 \leqq i \leqq r)$ such that $B \subset \bigcup_{1 \leqq i \leqq r} A_i$ and the following conditions are fulfilled. Let ${}_iF_f$ denote the restriction of F_f on A_i for $f \in C_c^\infty(G)$. Then ${}_iF_f \in \mathcal{E}_0(A_i \cap A')$ and the mapping $f \rightarrow {}_iF_f$ of $C_c^\infty(G)$ into $\mathcal{E}_0(A_i \cap A')$ is continuous for every i. Now if $f \in C_c^\infty(\omega)$, F_f is zero on A' outside B. Hence it is clear that

$$\sup_{H \in A'} |F_f(H;v)| \leqq \sum_{1 \leqq i \leqq r} \sup_{H \in A'_i} |F_f(H;v)| \qquad (v \in \mathfrak{H}),$$

where $A_i' = A_i \cap A'$. Therefore it follows that $F_f \in \mathcal{E}_0(A')$ and the mapping $f \rightarrow F_f$ of $C_c^\infty(\omega)$ into $\mathcal{E}_0(A')$ is continuous. All the statements of Theorem 2 are now obvious.

The following lemma is an immediate consequence of Theorem 2. Let dh denote the Haar measure on A.

LEMMA 17. *Let g be a measurable function on A which is bounded on every compact set. Then the mapping*

$$f \rightarrow \int_A F_f(h) g(h)\, dh \qquad (f \in C_c^\infty(G))$$

is a distribution on G.

This holds in particular if g is a character of A.

5. The main theorems. Let $\mathfrak{Z}$ denote the center of $\mathfrak{B}$. Then from Lemma 18 of [4(c)] there exists an isomorphism γ' of $\mathfrak{Z}$ into $S(\mathfrak{h})$ such that

$$z - \partial(\gamma'(z)) \in \sum_{\alpha \in P} \mathfrak{B} X_\alpha \qquad (z \in \mathfrak{Z}).$$

THEOREM 3. *Define F_f as in Theorem 2. Then*

$$F_{zf} = \partial(\gamma'(z)) F_f$$

for $f \in C_c^\infty(G)$ and $z \in \mathfrak{Z}$.

Fix a point $h_0 \in A'$ and let ω be a bounded open subset of G. Then as we saw during the proof of Lemma 14, there exists an open connected neighborhood B of h_0 in A' and a compact set Ω_0^* in G^* with the following property. If $xhx^{-1} \in \omega$ for some $h \in B$ and $x \in G$, then $x^* \in \Omega_0^*$. Therefore

$$F_g(h) = \Delta'(h) \int_{\Omega_0^*} g(h^{x^*})\, dx^* \qquad (h \in B, g \in C_c^\infty(\omega)).$$

Let Ω^* be a compact neighborhood of Ω_0^* in G^*. Normalize the Haar measures dx and dh on G and A, respectively, in such a way that

$$\int_G \beta(x)\,dx = \int_{G^*} dx^* \int_A \beta(xh)\,dh \qquad (\beta \in C_c(G)),$$

and select $\alpha \in C_c^\infty(G)$ such that $\int \alpha(xh)\,dh = 1$ if $x^* \in \Omega^*$ $(x \in G)$. Then if $f \in C_c^\infty(\omega)$ and $z \in \mathfrak{Z}$, it is obvious that

$$F_{zf}(h) = \Delta'(h) \int_G \alpha(x) f(xhx^{-1}; z)\,dx \qquad (h \in B).$$

Now we use the notation of [4(c), § 7] and put $f(x\colon h) = f(xhx^{-1})$ $(x \in G, h \in B)$. Then it follows from Lemma 23 of [4(c)] that

$$z = \Gamma_h(1 \times \beta_h(z)) + \sum_{1 \leqq i \leqq N} a_i(h) \Gamma_h(b_i \times u_i) \qquad (h \in B),$$

where $b_i \in \mathfrak{B}\mathfrak{g}, u_i \in \mathfrak{H}$ and a_i are analytic functions on B. Since $\mathfrak{B}\mathfrak{g}$ is the direct sum of $\mathfrak{S}'$ and $\mathfrak{B}\mathfrak{h}$ and $\Gamma_h(\mathfrak{B}\mathfrak{h} \times \mathfrak{H}) = \{0\}$, we may assume that $b_i \in \mathfrak{S}'$ and u_i $(1 \leqq i \leqq N)$ are linearly independent. Then since $z^h = z$, it follows from Lemma 22 of [4(c)] that $b_i^h = b_i$ $(h \in A)$. Therefore

$$f(xhx^{-1}; z) = f(x\colon h; \beta_h(z)) + \sum_{1 \leqq i \leqq N} a_i(h) f(x; b_i\colon h; u_i) \qquad (h \in B, x \in G)$$

and

$$F_{zf}(h) = \Delta'(h) \int_G \alpha(x) f(x\colon h; \beta_h(z))\,dx + \sum_{1 \leqq i \leqq N} a_i(h) \Delta'(h) \int_G \alpha(x; b_i^*) f(x\colon h; u_i)\,dx$$

for $h \in B$. (Here b_i^* is the adjoint of b_i). We now claim that

$$\int \alpha(x; b_i^*) f(x\colon h; u_i)\,dx = 0 \qquad (1 \leqq i \leqq N, h \in B).$$

It is clear that for a fixed h, $f(x\colon h; u_i)$ depends only on x^*. Hence it would be enough to prove that

$$\int_A \alpha(xh; b_i^*)\,dh = 0$$

if $x^* \in \Omega_0^*$. Choose a point $x_0 \in G$ such that $x_0^* \in \Omega_0^*$ and let U be an open neighborhood of 1 in G such that $(x_0U)^* \subset \Omega^*$. Then it follows from the definition of α that

$$\int_A \alpha(x_0yh)\,dh = 1 \qquad (y \in U).$$

Put $\alpha(x:h) = \alpha(xh)$ $(x \in G, h \in A)$. It is obvious that $(b_i^*)^h = b_i^*$ $(h \in A)$ and therefore $\alpha(x; b_i^*: h) = \alpha(xh; b_i^*)$. Therefore

$$\int_A \alpha(x_0 h; b_i^*)\, dh = \int_A \alpha(x_0; b_i^*: h)\, dh = 0$$

since $b_i^* \in \mathfrak{B}\mathfrak{g}$ and $\int \alpha(x_0 y: h)\, dh = 1$ for $y \in U$. This proves that

$$F_{zf}(h) = \Delta'(h) \int_G \alpha(x) f(x: h; \beta_h(z))\, dx \qquad (h \in B).$$

On the other hand, Theorem 2 of [4(c)] gives us a formula for $\beta_h(z)$. Define d as in this theorem. It follows easily from Lemma 7 of [4(c)] that $\operatorname{conj} \eta_\alpha(h^{-1}) = \eta_{\theta\alpha}(h)$ for $\alpha \in P$ and $h \in A$. Now if[9] $\alpha \in P_+$, the same holds for $-\theta\alpha$. Hence if $P' = P_0 \cup P_-$ (see [4(h), § 5] for notation), it is clear that

$$\operatorname{conj} \Delta'(h) = \prod_{\alpha \in P} (1 - \eta_{\theta\alpha}(h)) = (-1)^{r'} \prod_{\alpha \in P'} \eta_\alpha(h) \Delta'(h) \qquad (h \in A),$$

where r' is the number of roots in P'. Therefore

$$\begin{aligned} |d(h)| &= \Big| \prod_{\alpha \in P} (\eta_\alpha(h^{-1}) - 1)(\eta_\alpha(h) - 1) \Big| \\ &= \Big| \prod_{\alpha \in P_+} \eta_\alpha(h) \Big| \, |\Delta'(h)|^2 = (-1)^{r'} \Big| \prod_{\alpha \in P_+} \eta_\alpha(h) \Big| \prod_{\alpha \in P'} \eta_\alpha(h) \Delta'(h)^2. \end{aligned}$$

But

$$\operatorname{conj} \prod_{\alpha \in P_+} \eta_\alpha(h) = \prod_{\alpha \in P_+} \eta_{\theta\alpha}(h^{-1}) = \prod_{\alpha \in P_+} \eta_\alpha(h),$$

and so

$$|d(h)| = \pm \prod_{\alpha \in P} \eta_\alpha(h) \Delta'(h)^2.$$

Put $\rho = \frac{1}{2} \sum_{\alpha \in P} \alpha$ and select an open connected neighborhood $\mathfrak{h}_1$ of zero in $\mathfrak{h}_0$ such that $B_1 = h_0 \exp \mathfrak{h}_1 \subset B$. Then it is clear that

$$|d(h_0 \exp H)|^{\frac{1}{2}} = \epsilon e^{\rho(H)} \Delta'(h_0 \exp H) \qquad (H \in \mathfrak{h}_1),$$

where ϵ is a constant such that $\epsilon^4 = 1$. Therefore, it follows from Theorem 2 of [4(c)] that $\beta(z) = (\Delta')^{-1} \partial(\gamma'(z)) \circ \Delta'$ on B_1 and so

$$\begin{aligned} F_{zf}(h) &= \int \alpha(x) f(x: h; \partial(\gamma'(z)) \circ \Delta')\, dx \\ &= F_f(h; \partial(\gamma'(z))) \qquad (h \in B_1). \end{aligned}$$

This proves that F_{zf} and $\partial(\gamma'(z)) F_f$ coincide at h_0, and hence the theorem is established.

Put

$$\Delta_+'(h)=\prod_{\alpha\in P_+}(1-\eta_\alpha(h^{-1})),\qquad \Delta_0'(h)=\prod_{\alpha\in P_0}(1-\eta_\alpha(h^{-1}))\qquad (h\in A).$$

Then $\Delta_+'(h)$ is real since

$$\operatorname{conj}\Delta_+'(h)=\prod_{\alpha\in P_+}(1-\eta_{.\alpha}(h))=\prod_{\alpha\in P_+}(1-\eta_\alpha(h^{-1}))=\Delta_+'(h)$$

LEMMA 18. *Let $\epsilon_+(h)$ $(h\in A')$ denote the sign of $\Delta_+'(h)$ and A'' the set of all points $h\in A$ where $\Delta_0'(h)\neq 0$. Then for any $f\in C_c^\infty(G)$, ϵ_+F_f can be extended to a function of class C^∞ on A''.*

We use the notation of the proof of Lemma 15. Then

$$F_f(\exp H)=\zeta(H)\phi_f(H)\qquad (H\in\mathfrak{h}_1').$$

Put $\pi_+=\prod_{\alpha\in P_+}\alpha\in S(\mathfrak{h})$. It is obvious that if $\mathfrak{h}_1$ is sufficiently small, $\Delta_+'(\exp H)/\pi_+(H)$ can be extended to an analytic function on $\mathfrak{h}_1$ which is nowhere zero and which takes the value 1 at $H=0$. Therefore, since $\pi_+(H)$ is also real for $H\in\mathfrak{h}_0$, it has the same sign as $\Delta_+'(\exp H)$ for $H\in\mathfrak{h}_1'$. Hence it follows from Theorem 3 of [4(h)] that ϵ_+F_f can be extended to a function of class C^∞ on $B\cap A''$, where $B=\exp\mathfrak{h}_1$.

Now h_0 being a fixed point in A'', we use the notation of the proof of Lemma 16. Then $F_f=\psi_{g_f}'$ on $B\cap A'$. Since Δ_2' is never zero on B, it is clear that ϵ_+ differs on B from the sign of

$$\prod_{\alpha\in P_1\cap P_+}(1-\eta_\alpha(h^{-1}))$$

only by a constant factor. Therefore, by applying the above result to Ξ_0, we can conclude that there exists an open neighborhood B_1 of h_0 in B such that $\epsilon_+\psi_{g_f}'$ can be extended to a function of class C^∞ on $B_1\cap A''$. Since $\epsilon_+F_f=\epsilon_+\psi_{g_f}'$ on $B_1\cap A'$ and A' is dense in A'', the assertion of the lemma is now obvious.

Define $\mathfrak{h}_1$ and ζ as in the proof of Lemma 15 and put[8] $\pi'=\prod_{\alpha\in P}\{\alpha+\langle\alpha,\rho\rangle\}$ and consider the differential operator $\partial(\pi')\circ\zeta$ on $\mathfrak{h}_1$. As usual we denote its local expression at zero by $(\partial(\pi')\circ\zeta)_0$.

LEMMA 19. $(\partial(\pi')\circ\zeta)_0=\partial(\pi)$.

Since

$$\Delta'(\exp H)=e^{-\rho(H)}\prod_{\alpha\in P}(e^{\alpha(H)/2}-e^{-\alpha(H)/2})\qquad (H\in\mathfrak{h}_1)$$

and $e^{\rho}\partial(\pi') \circ e^{-\rho} = \partial(\pi)$, it would be enough to prove that $(\partial(\pi) \circ \zeta_1)_0 = \partial(\pi)$, where

$$\zeta_1(H) = \prod_{\alpha \in P} g(\alpha(H)) \qquad (H \in \mathfrak{h}_1)$$

and g denotes the entire function $(e^{t/2} - e^{-t/2})/t$ of the complex variable t. Then

$$\zeta_1 = 1 + \sum_{k \geqq 1} p_k,$$

where p_k is a homogeneous polynomial in $S(\mathfrak{h})$ of degree k and the above series converges to ζ_1 in some neighborhood $\mathfrak{h}_2$ of zero in $\mathfrak{h}_1$. Let W be the Weyl group of $\mathfrak{g}$ with respect to $\mathfrak{h}$. Then ζ_1 can be regarded as a holomorphic function on some complex neighborhood U of zero in $\mathfrak{h}$, and we may assume that $sU = U$ $(s \in W)$ and the above series converges to ζ_1 on U. Then since $\zeta_1(sH) = \zeta_1(H)$ $(s \in W)$, it follows that $p_k{}^s = p_k$ $(s \in W, k \geqq 1)$. Moreover, if f is any homogeneous element in $S(\mathfrak{h})$, it is obvious that

$$f(0;\partial(\pi) \circ \zeta_1) = f(0;\partial(\pi)) + \sum_{1 \leqq k \leqq r} f(0;\partial(\pi) \circ p_k),$$

where r is the degree of π. But it follows from Lemma 18 of [4(g)] that $f(0;\partial(\pi) \circ p_k) = 0$, and so $f(0;\partial(\pi) \circ \zeta_1) = f(0;\partial(\pi))$. Hence, if $(\partial(\pi) \circ \zeta_1)_0 - \partial(\pi) = \partial(q)$ $(q \in S(\mathfrak{h}))$, then[8] $\langle p, q\rangle = 0$ for all $p \in S(\mathfrak{h})$, and therefore (see [4(g), § 2]) $q = 0$. This proves the assertion of the lemma.

We say that the Cartan subgroup A is fundamental if $\mathfrak{h}_0$ is fundamental in $\mathfrak{g}_0$ (see [4(h), § 8]).

THEOREM 4. *We can select a neighborhood B of 1 in A with the following property. Suppose A_1 is a connected component of $A' \cap B$ whose closure contains 1. Then there exists a real number c such that*

$$\operatorname*{Lim}_{h \to 1} F_f(zh;\partial(\pi')) = cf(z) \qquad (h \in A_1)$$

for all $f \in C_c{}^{\infty}(G)$ and $z \in Z$. Moreover, $c = 0$ if A is not fundamental.

If $z = 1$, our statement is an immediate consequence of Lemma 19 and the fact that

$$F_f(\exp H) = \zeta(H)\phi_{\bar{f}}(H) \qquad (H \in \mathfrak{h}_1{}'),$$

if we take into account Theorem 2 of [4(i)]. For any arbitrary $z \in Z$, write $f_z(x) = f(zx)$ $(x \in G)$. Then

$$\operatorname*{Lim}_{h \to 1} F_f(zh;\partial(\pi')) = \operatorname*{Lim}_{h \to 1} F_{f_z}(h;\partial(\pi')) = cf_z(1) = cf(z) \qquad (h \in A_1).$$

THEOREM 5. *Suppose A is fundamental and $A_1, A_2, \cdots, A_r$ are all* *the distinct connected components of* $A' \cap B$ *whose closures contain* 1. *Let* c_i *be the real number of Theorem* 4 *corresponding to* A_i. *Then* $c_1 + c_2 + \cdots + c_r \neq 0$.

This follows immediately from Theorem 3 of [4(i)].

Note added on August 3, 1957. Recently I have been able to prove that $c_1 = c_2 = \cdots = c_r$ in Theorem 5. Since the normalization of the measure dx^* in Theorem 2 is arbitrary, only the sign of c_1 is of interest. Assuming that $\mathfrak{h}_0$ is fundamental, let p_+ and p_0 denote the number of roots in P_+ and P_0, respectively. Then p_+ is even and, if $q = p_0 + \frac{1}{2}p_+$, the sign of c_1 is $(-1)^q$.

Columbia University,
New York, N.Y.

REFERENCES.

[1] G. Birkhoff, *Ann. of Math.*, vol. 38 (1937), pp. 526-532.

[2] C. Chevalley, (a) *Theory of Lie Groups*, Princeton University Press, 1946.
(b) *Amer. Jour. Math.*, vol. 63 (1941), pp. 785-793.

[3] I. M. Gelfand and M. I. Graev, *Doklady Akad. Nauk. SSSR N. S.*, vol. 92 (1953), pp. 461-464.

[4] Harish-Chandra, (a) *Trans. Amer. Math. Soc.*, vol. 76 (1954), pp. 234-253.
(b) ———, vol. 76 (1954), pp. 485-528.
(c) ———, vol. 83 (1956), pp. 98-163.
(d) *Amer. Jour. Math.*, vol. 77 (1955), pp. 743-777.
(e) ———, vol. 78 (1956), pp. 1-41.
(f) ———, vol. 78 (1956), pp. 564-628.
(g) ———, vol. 79 (1957), pp. 87-120.
(h) ———, vol. 79 (1957), pp. 193-257.
(i) ———, vol. 79 (1957), pp. 653-686.
(j) *Proc. Nat. Acad. Sci. U.S.A.*, vol. 42 (1956), pp. 538-540.

[5] K. Iwasawa, *Ann. of Math.*, vol. 50 (1949), pp. 507-557.

[6] L. Schwartz, *Theorie des distributions I*, (1950), Paris, Hermann.

[7] A. Weil, *L'integration dans les groupes topologiques et ses applications*, Paris, Hermann.

DIVISORS AND ENDOMORPHISMS ON AN ABELIAN VARIETY.*

By SERGE LANG.

We consider here the fundamental theorem on the algebra of endomorphisms of an abelian variety dealing with the existence of a positive definite quadratic form defined by means of the trace. We shall give a direct proof on abelian varieties for Weil's formula $\sigma(\xi\xi') > 0$, which will exhibit the positivity as a formal consequence of the definitions. Weil's method is to show that the trace can be expressed as an intersection number (Proposition 20 of [6], No. 47). However, even on a Jacobian, his proof that $\sigma(\xi)$ coincides with the penultimate coefficient of the characteristic polynomial is somewhat indirect (Theorem 34 of [6], No. 66). In the present exposition, this will be straightforward, and we shall obtain a simple representation of the trace as an intersection number canonically determined by a given projective embedding of the abelian variety A, or as Weil would say, a polarization of A [8].

More generally, if α_i $(i=1,\cdots,d)$ are endomorphisms of A and m_i $(i=1,\cdots,d)$ are integers, then we give an expression for the coefficients of the homogeneous polynomial $\nu(m_1\alpha_1+\cdots+m_d\alpha_d)$ in terms of intersection numbers canonically determined by the α_i and the given polarization.

Our arguments are based on only two properties of abelian varieties: The theorem of the square (see below), and the fact that a divisor which is $\equiv 0$ is numerically equivalent to 0. (Weil [6], No. 62 and Morikawa [5], Lemma 7.) For the convenience of the reader, we reproduce in an appendix a simple proof of Weil for this fact.

We shall begin by defining a bilinear mapping of the endomorphisms of A into the Neron-Severi group of divisors $N(A)$, given by the formula $D_X(\alpha,\beta) \equiv (\alpha+\beta)^{-1}(X) - \alpha^{-1}(X) - \beta^{-1}(X)$. The properties of the trace are then reflected from analogous properties of our divisorial pairing. We shall take X to be a positive non-degenerate divisor. We call a class of divisors in $N(A)$ positive if a suitable positive integral multiple of it contains a positive divisor. The formula $\mathrm{tr}(\alpha\alpha') > 0$ then comes from the fact that $D_X(\alpha,\alpha)$ is positive.

We then discuss a pairing of endomorphisms into the group $N_1(A)$ of

---

* Received February 15, 1957.

1-cycles modulo those which are numerically equivalent to 0. It is dual to the above, and is defined by the formula $Z_C(\alpha,\beta)=(\alpha+\beta)(C)-\alpha(C)-\beta(C)$. Properties of $D_X(\alpha,\beta)$ are easily transferred to properties of $Z_C(\alpha,\beta)$. We introduce the Pontrjagin product between cycles of A, which is dual to the intersection product, and are then able to recover all the numerical statements contained in Weil [6] (for instance, the Lefschetz fixed point formula for curves). Some questions concerning the Pontrjagin product remain unanswered, principally those concerning the more precise duality which exists between this product and the ordinary intersection product.

The above section dealing with 1-cycles is not used in the section following it, where we analyse the positivity of divisor classes in $N(A)$. We generalize results of Morikawa [5], except that we work only in the tensor product of $N(A)$ with the rational numbers, and do not consider integrality questions related to the positivity. For instance, let Y be a divisor and suppose that there exists an integer $m>0$ and a divisor $Y_1>0$ such that $mY\equiv Y_1$. Does there exist a divisor $Y_2>0$ such that $Y\equiv Y_2$?

Finally, we have pointed out how one can see directly on an abelian variety that the characteristic roots of the Frobenius endomorphism all have absolute value $q^{\frac{1}{2}}$ without having to go through the theory of curves. Together with the Lefschetz fixed point formula, this gives a more natural proof for the Riemann hypothesis for curves.

1. Applications of the theorem of the square.

For the rest of this paper, A, B will denote abelian varieties and $X,Y,Z,\cdots$ will be divisors on A or B. We denote by $H(A,B)$ the module of homomorphisms of A into B, and by $H(A)$ the ring of endomorphisms of A. The tensor products with $\boldsymbol{Q}$ will be denoted by $H_{\boldsymbol{Q}}(A,B)$ and $H_{\boldsymbol{Q}}(A)$ respectively. If $\alpha\in H_{\boldsymbol{Q}}(A,B)$ and $\nu(\alpha)\neq 0$, then there is an element β of $H_{\boldsymbol{Q}}(B,A)$ such that $\beta\alpha$ is the identity. We write $\beta=\alpha^{-1}$.

We denote by $\hat{A}$ the dual variety (Picard variety) of A. If X is a divisor on A, algebraically equivalent to 0, then $\mathrm{Cl}(X)$ denotes the point on $\hat{A}$ associated with the linear equivalence class of X. The theorem of the square states that the mapping

$$\varphi_X: u\rightarrow \mathrm{Cl}(X_u-X)$$

is a homomorphism of A into $\hat{A}$. By definition, $X\equiv 0$ if and only if $\varphi_X=0$.

We let $D(A)$ be the group of divisors on A, and $D_l(A)$ the subgroup of divisors linearly equivalent to 0. Let $\alpha\in H(A,B)$. Let X be a divisor on B. Then $\alpha^{-1}(X)$ may not be defined, but if t is a generic point of B, then $\alpha^{-1}(X_t)$ is always defined. Furthermore, if X is algebraically equivalent to 0 on B, then $X_t \sim X$, and if $X \sim 0$ on B and $\alpha^{-1}(X)$ is defined, then $\alpha^{-1}(X) \sim 0$ on A. If V is a variety, we denote by $D_a(V)$ the group of divisors algebraically equivalent to 0 on V. Then the above remarks show that α induces a linear map α^{-1} of $D_a(B)/D_l(B)$ into $D_a(A)/D_l(A)$. (Later we shall use the terminology of the Picard variety, and we call this map the transpose of α.)

We denote by $N(A)$ the factor group of $D(A)$ by the subgroup of divisors of A which are $\equiv 0$. Then α will also induce an inverse mapping α^{-1} of $N(B)$ into $N(A)$ as follows. We contend that if t and u are generic points of B then $\alpha^{-1}(X_t) \equiv \alpha^{-1}(X_u)$. To prove this, we first state a lemma explicitly.

Lemma. *Let $\lambda \colon A \to B$ be a homomorphism, X a divisor on B, v a point of A such that $\lambda^{-1}(X_{\lambda v})$ is defined. Assume also that $\lambda^{-1}(X)$ is defined. Then $(\lambda^{-1}(X))_v = \lambda^{-1}(X_{\lambda v})$.*

Proof. The translation $(v, \lambda v)$ on $A \times B$ leaves the graph of λ fixed. It moves $\lambda^{-1}(X)$ on its translate by v, and moves X on its translate by λv. The lemma is then obvious.

Returning to the proof of our contention, we let v be a generic point of A, independent of t and u. Then $\alpha^{-1}(X_{t+\alpha v})$ and $\alpha^{-1}(X_{u+\alpha v})$ are defined, and a trivial computation starting with the definitions, together with the theorem of the square proves our contention.

Given a divisor X on B, and $\alpha \in H(A,B)$, then from the theorem of the square, we know that $X_t \equiv X$, and hence the class $\alpha^{-1}(X_t)$ in $N(A)$ depends only on X and α and not on the auxiliary generic point t. By an abuse of language, we shall denote this class by $\alpha^{-1}(X)$. The context will always make clear whether we deal with a class in $N(A)$, or whether we deal with a divisor X in $D_a(B)$, in which case $\alpha^{-1}(X)$ will mean the linear equivalence class in $D_a(A)/D_l(A)$.

The following theorem and its proof are directly inspired from Weil's Proposition 31, [6], No. 73. For the special case of elliptic curves, see Hasse [4].

Theorem 1. *Let $\alpha, \beta \in H(A,B)$. Define*

$$D_X(\alpha,\beta) \equiv (\alpha+\beta)^{-1}(X) - \alpha^{-1}(X) - \beta^{-1}(X),$$

this being an element of $N(A)$. Let m, n be integers. Then

$$(m\alpha + n\beta)^{-1}(X) \equiv m^2\alpha^{-1}(X) + mnD_X(\alpha,\beta) + n^2\beta^{-1}(X).$$

Proof. The proof will be carried out in three steps. Throughout, we let $s_n\colon B\times\cdots\times B\to B$ be the sum on the product of B n-times with itself, and we let $p_i\colon B\times\cdots\times B\to B$ be the projection on the i-th factor.

1.) $X\equiv 0$ if and only if $s_n^{-1}(X)\sim\sum p_i^{-1}(X)$.

For simplicity take $n=2$. Then for u generic on B, we have

$$s_2^{-1}(X)\cdot(B\times u)=X_{-u}\times u.$$

Hence $[s_2^{-1}(X)-(X\times B)]$. $(B\times u)=(X_{-u}-X)\times u$. If $X\equiv 0$, then this is linearly equivalent to 0, and hence we can write

$$s_2^{-1}(X)\sim(X\times B)+(B\times Y)$$

for some divisor Y on B. By symmetry, we must have $Y\sim X$. The converse is equally clear.

2.) If $X\equiv 0$ then

$$(\alpha+\beta)^{-1}(X)\sim\alpha^{-1}(X)+\beta^{-1}(X).$$

Let $\lambda\colon A\to B\times B$ be the composite map (α,β), so we have $\lambda u=(\alpha u,\beta u)$ for u in A. Then $s_2\lambda=\alpha+\beta$, and $p_i\lambda=\alpha$ or β according as $i=1$ or 2. Using the formula $(fg)^{-1}=g^{-1}f^{-1}$ which is applicable in the present case, together with step 1, we get what we want.

3.) We finish the proof in this step. Let X be arbitrary. Using the above lemma, we get

$$((m\alpha+n\beta)^{-1}(X))_u-(m\alpha+n\beta)^{-1}(X)=(m\alpha+n\beta)^{-1}(X_{(m\alpha+n\beta)u}-X).$$

For any $v\in B$, $X_v-X\equiv 0$. Using step 2 and making repeated use of the theorem of the square, we see that this expression is linearly equivalent to

$$(1)\qquad m^2\alpha^{-1}(X_{\alpha u}-X)+mn\alpha^{-1}(X_{\beta u}-X)+mn\beta^{-1}(X_{\alpha u}-X)+n^2\beta^{-1}(X_{\beta u}-X).$$

Let $Z=\alpha^{-1}(X_{\beta u}-X)+\beta^{-1}(X_{\alpha u}-X)$. To prove our theorem, it suffices to shrow that $Z\sim D_X(\alpha,\beta)_u-D_X(\alpha,\beta)$. One sees this by putting $m=n=1$ in formula (1), and using the lemma.

To go further, it is convenient to use the language and formalism of the Picard variety. (At present, a complete exposition is not yet published. Some of it will be in Chow [3], and the commutative diagrams below are due to Weil. See also Morikawa [5].) Given a homomorphism $\alpha\in H(A,B)$, then one has an induced contravariant mapping on the Picard varieties,

${}^t\alpha\colon \hat{B} \to \hat{A}$, which we shall call the *transpose* of α. We shall use constantly the linearity property

$$(2) \qquad {}^t(\alpha + \beta) = {}^t\alpha + {}^t\beta,$$

which is essentially step 2 in the proof of Theorem 1. If $\theta_A\colon A \to \hat{\hat{A}}$ denotes the canonical map of A onto its double dual, and X is a divisor on A, then the following diagram is commutative:

(3)

$$\begin{tikzcd} A \arrow[rr, "\varphi_X"] \arrow[dr, "\theta_A"'] & & \hat{A} \\ & \hat{\hat{A}} \arrow[ur, "{}^t\varphi_X"'] & \end{tikzcd}$$

If $\alpha \in H(A, B)$ and if Y is a divisor on B, then the following diagram is commutative:

(4)

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "\varphi_{\alpha^{-1}(Y)}"'] & B \arrow[d, "\varphi_Y"] \\ \hat{A} & \hat{B} \arrow[l, "{}^t\alpha"] \end{tikzcd}$$

i.e., we have $\varphi_{\alpha^{-1}(Y)} = {}^t\alpha \circ \varphi_Y \circ \alpha$.

It follows just as in Theorem 1 that

$$(5) \qquad \varphi_{D_X(\alpha,\beta)} = {}^t\alpha \circ \varphi_X \circ \beta + {}^t\beta \circ \varphi_X \circ \alpha$$

for any divisor X on B. Conversely, one might also use the present formalism to deduce the following generalization. If $\alpha_1, \cdots, \alpha_d$ are homomorphisms of A into B, and $m_1, \cdots, m_d$ are integers, then

$$(6) \qquad (m_1\alpha_1 + \cdots + m_d\alpha_d)^{-1}(X) \equiv \tfrac{1}{2} \sum m_i m_j D_X(\alpha_i, \alpha_j),$$

the sum being taken for $i, j = 1, \cdots, d$, so that each term appears twice and we therefore divide by 2.

In addition, the linearity property of the transpose gives us immediately a bilinear map of $H(A, B)$ into $N(A)$, namely the class of $D_X(\alpha, \beta)$ obeys the rules:

D1. $\qquad D_X(\alpha + \beta, \gamma) \equiv D_X(\alpha, \gamma) + D_X(\beta, \gamma).$

D2. $\qquad D_X(\alpha, \beta) \equiv D_X(\beta, \alpha).$

D3. $$D_X(m\alpha, \beta) \equiv m D_X(\alpha, \beta).$$

D4. $$D_X(\alpha, \alpha) \equiv 2\alpha^{-1}(X).$$

Condition D4 is due to the commutative diagram (4). The others are clear.

For the rest of this paper, we shall take $B = A$. Following Morikawa [5], we say that a divisor X on A is *non-degenerate* if the kernel of φ_X is finite. As Weil has shown [7], it is practically obvious that if X is positive and non-degenerate, then a suitable positive multiple of X is ample, i.e., becomes a hyperplane section in a projective embedding of A. From now on, *X will denote a positive non-degenerate divisor on A, whose class in $N(A)$ will remain fixed throughout.* It then follows that for any $\alpha \neq 0$ in $H(A)$, there exists an integer $m > 0$ and a divisor $Y > 0$ such that $m\alpha^{-1}(X) \equiv Y$. Condition D4 can thus be interpreted as a condition of positive definiteness.

Relative to our divisor X, we define an involution on $H_{\boldsymbol{Q}}(A)$ by letting $\alpha' = \varphi_X^{-1} \circ {}^t\alpha \circ \varphi_X$. The commutativity relations (3) and (4) show that $\alpha \rightarrow \alpha'$ is an anti-automorphism, i.e., that

$$(\alpha + \beta)' = \alpha' + \beta', \qquad (\alpha')' = \alpha, \qquad (\alpha\beta)' = \beta'\alpha', \qquad \delta' = \delta.$$

Our pairing $D_X(\alpha, \beta)$ in $N(A)$ can then be extended to a bilinear map of $H_{\boldsymbol{Q}}(A)$ into $N_{\boldsymbol{Q}}(A)$. We can rewrite formula (5) in the form

$$\varphi_{D_X(\alpha,\beta)} = \varphi_X(\alpha'\beta + \beta'\alpha). \tag{7}$$

It will be convenient to introduce still another symbol. We define

$$D_X(\alpha) \equiv D_X(\alpha, \delta) \equiv (\alpha + \delta)^{-1}(X) - \alpha^{-1}(X) - X.$$

If $\alpha \in H(A)$, then $\alpha \rightarrow D_X(\alpha)$ gives a linear map of $H(A)$ into $N(A)$ which can be extended to a $\boldsymbol{Q}$-linear map of $H_{\boldsymbol{Q}}(A)$ into $N_{\boldsymbol{Q}}(A)$.

We can supplement D1-D4 by more formulas which give the behavior of our pairing under multiplication, namely, for any divisor Y, we have

D5. $$D_X(\varphi_X^{-1}\, {}^t\alpha\varphi_Y\beta) \equiv D_Y(\alpha, \beta).$$

D6. $$D_X(\lambda\alpha, \lambda\beta) \equiv D_{\lambda^{-1}(X)}(\alpha, \beta).$$

D7. $$D_X(\alpha\lambda, \beta\lambda) \equiv \lambda^{-1} D_X(\alpha, \beta).$$

These formulas are direct consequences of the definitions and commutativity.

From D5 we deduce immediately formulas for $D_X(\alpha)$, namely,

D8. $$D_X(\alpha, \beta) \equiv D_X(\alpha'\beta).$$

D9. $$D_X(\alpha\beta, \gamma) \equiv D_X(\beta, \alpha'\gamma).$$

D10. $$D_X(\beta'\alpha\beta) \equiv \beta^{-1}D_X(\alpha).$$

D11. $$D_X(\alpha) \equiv D_X(\alpha').$$

The preceding formulas exhaust the formal behavior of our divisorial pairing, and we shall now turn to its application to the trace.

2. The trace. In this section, we use as our basic fact that if $X \equiv 0$, then X is numerically equivalent to 0. In an appendix, we shall reproduce a simple proof due to Weil, based only on the theorem of the square.

We consider divisors up to numerical equivalence, since we are concerned here with numerical statements. If Y is a divisor on A, then the intersection of Y with itself s times is understood to be up to numerical equivalence. If $t_1, \cdots, t_s$ are independent generic points, then $Y_{t_1} \cdot Y_{t_2} \cdots Y_{t_s}$ is an element of that class, for instance. We let r be the dimension of A. If C is any positive cycle of dimension 1 on A, then $\deg(X \cdot C) > 0$ because we have assumed X positive non-degenerate, hence essentially a hyperplane section of A.

In what follows, we shall also use the formula

$$\alpha^{-1}(Y_1 \cdot Y_2) = \alpha^{-1}(Y_1) \cdot \alpha^{-1}(Y_2),$$

which holds whenever both sides are defined. Generic translations will always insure that this is the case. Note also if $\mathfrak{a}$ is a 0-cycle, and $\nu(\alpha) \neq 0$, then

$$\deg(\alpha^{-1}(\mathfrak{a})) = \nu(\alpha)\deg(\mathfrak{a}).$$

From these remarks, we first note that if we intersect both sides of (6) with themselves r times ($r = \dim A$), then we recover immediately Weil's theorem that $\nu(m_1\alpha_1 + \cdots + m_d\alpha_d)$ as a function of $(m_1, \cdots, m_d)$ is a homogeneous polynomial of degree $2r$. Moreover, its coefficients are easily determined explicitly in terms of intersections of the $D_X(\alpha_i, \alpha_j)$.

We are particularly interested in the special case which yields the characteristic polynomial of an endomorphism. In Theorem 1 we take $m = 1$, and $\beta = \delta$. We get:

$$(\alpha + n\delta)^{-1}(X) \equiv n^2X + nD_X(\alpha) + \alpha^{-1}(X).$$

Again raising this equation to the r-th power, we get

$$\nu(\alpha + n\delta)\deg(X^{(r)}) = c_{2r}n^{2r} + c_{2r-1}n^{2r-1} + \cdots + c_0,$$

where $X^{(r)}$ denotes the class up to numerical equivalence of the intersection of X with itself r times, and the c_i are integers which are easily determined explicitly in terms of intersections of $\alpha^{-1}(X)$, X, and $D_X(\alpha)$. For instance, we have

$$c_{2r} = \deg X^{(r)}, \qquad c_{2r-1} = r \cdot \deg(X^{(r-1)} \cdot D_X(\alpha)), \qquad c_0 = \nu(\alpha) \deg X^{(r)}.$$

This shows that $\nu(\alpha + n\delta)$ is a polynomial in n with rational coefficients. In [6], No. 67-68, Weil gives a simple and direct argument showing that the characteristic polynomial is actually that obtained from an l-adic representation.

The trace of α, which we denote by $\operatorname{tr}(\alpha)$, is defined by the formula

$$\operatorname{tr}(\alpha) = r/\deg(X^{(r)}) \cdot \deg(X^{(r-1)} \cdot D_X(\alpha)).$$

From D5 we immediately get

$$\operatorname{tr}(\alpha'\beta) = r/\deg(X^{(r)}) \cdot \deg(X^{(r-1)} \cdot D_X(\alpha, \beta)).$$

The main properties of the trace are then directly traceable to the properties of the divisor class $D_X(\alpha, \beta)$.

On the algebra $H_{\boldsymbol{Q}}(A)$ over the rational numbers, we can define a scalar product (taking its value in $\boldsymbol{Q}$) by putting $(\alpha, \beta) = \operatorname{tr}(\alpha'\beta)$. We then have the usual properties of a bilinear form, whose quadratic form is positive definite, and in addition we have the multiplicative property $(\alpha\beta, \gamma) = (\beta, \alpha'\gamma)$. This follows immediately from the analogous properties of $D_X(\alpha, \beta)$. The strict positivity comes from the fact that for some integer $m > 0$, mX is a hyperplane section of A, and hence the class of $m\alpha^{-1}(X)$ in $N(A)$ contains a divisor $Y > 0$. As we have noted before, we must then have $\deg(X^{(r-1)} \cdot \alpha^{-1}(X)) > 0$. From D4 and the definition of (α, α) we conclude that $(\alpha, \alpha) > 0$.

We define the norm $\| \alpha \|$ as usual by $(\alpha, \alpha)^{\frac{1}{2}}$. Aside from the usual properties of a metric, we have in addition the following statements:

N1. $\| \alpha \| = \| \alpha' \|$

N2. $\| \alpha'\alpha \| = \| \alpha\alpha' \|$

N3. If $\alpha \neq 0$ and $\beta \neq 0$, then $\| \alpha\beta \| < \| \alpha \| \, \| \beta \|$.

The first two are clear from the commutativity of the trace. As to the third, we have

$$\| \alpha\beta \|^2 = \operatorname{tr}(\beta'\alpha'\alpha\beta) = \operatorname{tr}(\alpha'\alpha\beta\beta') = (\alpha'\alpha, \beta\beta') \leqq \| \alpha'\alpha \| \, \| \beta\beta' \|,$$

this last inequality being the Schwartz inequality. We are therefore reduced to proving the inequality $\| \alpha'\alpha \| < \| \alpha \|^2$. By definition we have $\| \alpha'\alpha \|^2 = \operatorname{tr}(\alpha'\alpha\alpha'\alpha) = \operatorname{tr}((\alpha\alpha')^2)$. Let ω_j be the characteristic roots of $\alpha\alpha'$. Then

ω_j^2 are the characteristic roots of $(\alpha\alpha')^2$. It is known, and we shall recall the proof in the next section, that the ω_j are totally real totally positive algebraic numbers. Our inequality is equivalent to $\sum \omega_j^2 < (\sum \omega_j)^2$ which is true in view of this fact.

As an application, we consider an abelian variety A defined over a finite field k with q elements, and assume that X is rational over k. Then one verifies trivially that if π is the Frobenius endomorphism relative to k, then $\pi\pi' = \pi'\pi = q\delta$. Hence in that case, $\| \pi \| = (2rq)^{\frac{1}{2}}$. Furthermore, $\operatorname{tr}(\pi) = \operatorname{tr}(\pi\delta) = (\pi, \delta)$ and by the Schwartz inequality we get

$$| \operatorname{tr}(\pi) | \leqq \| \pi \| \, \| \delta \| = 2rq^{\frac{1}{2}}.$$

For any integer n, we get $| \operatorname{tr}(\pi^n) | \leqq 2rq^{n/2}$. If ω_j are the characteristic roots of π, then ω_j^n are those of π^n. From this one sees easily that the absolute value of a characteristic root can be at most $q^{\frac{1}{2}}$. Since we have $\nu(\pi) = q^r$, the product of the characteristic roots of π must be equal to $\pm q^r$ Hence the absolute value of each one of the characteristic roots is exactly $q^{\frac{1}{2}}$.

3. A dual pairing.* We introduce a pairing of the endomorphisms of A into the group of 1-cycles on A modulo numerical equivalence which is dual to the divisorial pairing of Section 1. The symbol $\equiv$ will now denote numerical equivalence, and $N_i(A)$ denotes the factor group of i-cycles by those which are numerically equivalent to 0.

Let Z be a cycle on A. Let $\alpha \in H(A)$. As usual, we mean by $\alpha(Z)$ the intersection $\mathrm{pr}_2[\Gamma_\alpha \cdot (Z \times A)]$.

We shall be particularly interested in 1-cycles. Let C be a 1-cycle. If Y is a divisor on A, then we have the *transposition formula*

$$\deg(\alpha(C) \cdot Y) = \deg(C \cdot \overset{\prime\prime}{\alpha}{}^{-1}(Y)). \tag{8}$$

The easy proof runs as follows.

$$\begin{aligned} \deg(\alpha(C) \cdot Y) &= \deg\{\mathrm{pr}_2[(\Gamma_\alpha \cdot (C \times A)) \cdot (A \times Y)]\} \\ &= \deg\{((C \times A) \cdot \Gamma_\alpha) \cdot (A \times Y)\}, \end{aligned}$$

because the degree of a 0-cycle is preserved under projection. All that remains to be done is to use associativity, and then unwind the above expression with respect to Y, just as we have done with respect to C.

We can transfer to the 1-cycles properties of divisors by transposition. For $\alpha, \beta \in H(A)$ we define

$$Z_C(\alpha, \beta) \equiv (\alpha + \beta)(C) - \overset{\prime\prime}{\alpha}(C) - \beta(C), \qquad Z_C(\alpha) \equiv Z_C(\alpha, \delta),$$

---

* This section was added March 22, 1957.

these being elements of $N_1(A)$. We get trivially

$$\deg[Z_C(\alpha,\beta)\cdot Y] = \deg[C\cdot D_Y(\alpha,\beta)]. \tag{9}$$

This shows that $Z_C(\alpha,\beta)$ gives a bilinear map of $H(A)$ into $N_1(A)$, and D4 becomes $Z_C(\alpha,\alpha) \equiv 2\alpha(C)$. In addition, we obtain

$$(m\alpha + n\beta)(C) \equiv m^2\alpha(C) + mnZ_C(\alpha,\beta) + n^2\beta(C) \tag{10}$$

$$(\alpha + n\delta)(C) \equiv n^2 C + nZ_C(\alpha) + \alpha(C). \tag{11}$$

In order to apply a numerical calculus dual to the intersection calculus of cycles used in Section 2, we must define the Pontrjagin product of cycles on A as follows. Let V, W be two subvarieties of A. By $V \oplus W$ we shall denote the set theoretic sum of V and W taken in A. It is the variety consisting of all points $v + w$ with $v \in V$ and $w \in W$. There is a rational map $F\colon V \times W \rightarrow V \oplus W$ which may or may not be of finite degree. By $d(V, W)$ we denote the degree of F if it is finite, and 0 otherwise. Similarly, we define $d(V_1, \cdots, V_m)$ for any finite number of subvarieties of A to be the degree of the rational map from their product to their set theoretic sum if it is finite, and 0 otherwise. We denote by $V * W$ the cycle $d(V, W)(V \oplus W)$, and one sees immediately that $V * W = \mathrm{pr}_3[S\cdot(V \times W \times A)]$, where S is the graph of the sum $s_2\colon A \times A \rightarrow A$. Note that $V * W = 0$ if and only if the dimension of $V \oplus W$ is smaller than $\dim V + \dim W$. From the definitions, one also sees that the Pontrjagin product is associative, and that $V_1 * V_1 * \cdots * V_m = d(V_1, \cdots, V_m)(V_1 \oplus V_2 \oplus \cdots \oplus V_m)$. The product extends naturally to cycles by linearity, and if Z_1, Z_1 are two cycles, then

$$Z_1 * Z_2 = \mathrm{pr}_3[S\cdot(Z_1 \times Z_2 \times A)].$$

From the fact that the expression on the right is built up from the standard operations of intersection theory, we see that the Pontrjagin product defines a commutative ring structure on the graded module $\sum N_i(A)$.

Let $\alpha \in H(A)$. Then α induces an endomorphism of our ring, i.e., we have

$$\alpha(V_1 * V_2 * \cdots * V_m) = \alpha(V_1) * \alpha(V_2) * \cdots * \alpha(V_m). \tag{12}$$

This is easily seen by applying the definitions. We are now in a position to use the same method as in Section 2 to get an expression for the characteristic polynomial $\nu(\alpha + n\delta)$, except that we use the Pontrjagin product instead of the intersection product. We are mostly interested in the trace. Raising both sides of (11) to the r-th power, using (12), we get

$$\mathrm{tr}(\alpha) = r/d(C, \cdots, C)\cdot\deg[C^{*(r-1)} * Z_C(\alpha)], \tag{13}$$

provided we take for C a curve which generates A. Here, $C^{*(r-1)}$ means the

Pontrjagin product of C with itself $(r-1)$ times, and the degree is defined to be the coefficient of A appearing in the expression on the right. It is convenient to transform this expression into an intersection number. Whenever V and W have complementary dimesion, we have

$$(14) \qquad d(V, W) = \deg(V \cdot W^{-}) = \deg(V^{-} \cdot W),$$

denoting by V^{-} the transform of V by the map sending each point into its inverse. This is a restatement of an elementary result concerning algebraic groups (Weil [6], No. 13, Cor. 2 of Th. 4). If V is a divisor, then $V^{-} \equiv V$, say, by taking $\alpha = -\delta$ in the commutative diagram (4), and hence the expression for the trace becomes

$$(15) \qquad \operatorname{tr}(\alpha) = r/d(C, \cdot \cdot \cdot, C) \cdot \deg(C^{*(r-1)} \cdot Z_C(\alpha)).$$

We have thus recovered all the numerical results contained in Weil's treatise on Abelian varieties. Consider the special case where $A = J$ is the Jacobian of a curve C. Then $C^{*(r-1)} = (g-1)!\Theta$, and $d(C, \cdot \cdot \cdot, C) = g!$. Using the transposition formula we get

$$(16) \qquad \operatorname{tr}(\alpha) = \deg(D_{\Theta}(\alpha) \cdot C).$$

We remark that if we had tried to obtain this directly from the expression of the trace obtained by the ordinary intersection product, we would have needed the extra information that

$$\Theta^{(g-1)} \equiv (g-1)!C \text{ and } \deg(\Theta^{(g)}) = g!.$$

Remarkably enough, there does not seem to be an easy proof available for this fact. Such a proof would require a closer analysis of the relations which exist between the ordinary and the Pontrjagin products of cycles.

Formula (16) allows us to recover the Lefschetz fixed point formula (and hence the Riemann hypothesis for curves), for we can now use the proof given by Weil ([6], No. 47) which is quite transparent. For the convenience of the reader, we reproduce this proof. If T is a correspondence on C (i.e., a 1-cycle on $C \times C$), we let τ be the associated endomorphism of J. The fixed point formula states that

$$\deg(T \cdot \Delta) = d(T) - \operatorname{tr}(\tau) + d'(T).$$

We let s_2 be the sum on $J \times J$, and consider the following diagram:

$$\begin{tikzcd}
C \times C \arrow[r, "f_2"] & J \times J \arrow[r, "(\tau, \delta)"] & J \times J \arrow[r, "s_2"] & J \\
C \arrow[u, "h_i"] \arrow[r, "f"'] & J \arrow[u, "H_i"'] & &
\end{tikzcd}$$

Here, f is the canonical mapping, f_2 is the product of f with itself, and h_i, H_i $(i=1,2,3)$ are described as follows: For $i=1$ we take the diagonal mapping. For the others, we may assume that we have a point P on C such that $f(P)=0$ is the origin on J. Then h_2 maps C on $P\times C$ and h_3 maps C on $C\times P$. Similarly, H_2 maps J on $0\times J$ and H_3 maps J on $J\times 0$. Then the square is commutative. Put $\lambda=(\tau,\delta)$. Then $f_2^{-1}\lambda^{-1}s_2^{-1}(-\Theta)$ is a correspondence T on $C\times C$ whose associated endomorphism is precisely τ. (Of course, in taking our inverse mappings, we first make a generic translation on Θ.) Furthermore, we have

$$s_2\lambda H_1=\tau+\delta,\qquad s_2\lambda H_2=\delta,\qquad s_2\lambda H_3=\tau.$$

From the commutativity, it is then obvious that

$$\deg[(\tau+\delta)^{-1}(-\Theta)\cdot C]=\deg(T\cdot\Delta),\qquad \deg[\tau^{-1}(-\Theta)\cdot C]=d(T),$$
$$\deg(-\Theta\cdot C)=d'(T).$$

This concludes the proof.

4. Positive endomorphisms. We shall say that an element α in $H_Q(A)$ is *symmetric* if $\alpha=\alpha'$. These elements form a subspace $S_Q(A)$ of $H_Q(A)$ over the rational numbers. We have a $\boldsymbol{Q}$-linear map $D_X\colon S_Q(A)\to N_Q(A)$, defined by $\alpha\to D_X(\alpha)$. It is in fact an isomorphism, and we shall define its inverse $\Phi_X\colon N_Q(A)\to S_Q(A)$ as follows. If Y is a divisor representing a class in $N(A)$ then we put $\Phi_X(Y)=\frac{1}{2}\varphi_X^{-1}\varphi_Y$. The map $Y\to\Phi_X(Y)$ clearly induces a $\boldsymbol{Q}$-linear map of $N_Q(A)$ into $H_Q(A)$. The commutativity relations (3) and (4) show that it is into $S_Q(A)$, i.e., that $\varphi_X^{-1}\varphi_Y$ is symmetric. From (7), we see that $D_X\Phi_X$ and Φ_XD_X are both equal to the identity, and hence are isomorphisms.

If Y is a divisor representing a class in $N(A)$, we shall write $\alpha\leftrightarrow Y$ to mean that $\alpha=\Phi_X(Y)$.

PROPOSITION 1. *Let α be a symmetric element of $H_Q(A)$, and suppose $\alpha\leftrightarrow Y$. Let λ be any element of $H_Q(A)$. Then $\lambda'\alpha\lambda\leftrightarrow\lambda^{-1}(Y)$. In particular, $\lambda'\lambda\leftrightarrow\lambda^{-1}(X)$.*

Proof. This is a reformulation of D10.

We shall say that an element of $H_Q(A)$ is *positive* (relative to the divisor X) if it is symmetric, and if there exists an integer $m>0$ such that the class of $D_X(m\alpha)$ in $N(A)$ contains a divisor $Y>0$. We then write $\alpha>0$.

PROPOSITION 2. *Let α be symmetric.*

a.) *If $\alpha \geqq 0$, and λ is any element of $H_Q(A)$ then $\lambda'\alpha\lambda \geqq 0$.*

b.) *If $\lambda \in H_Q(A)$ and $\lambda \neq 0$, then $\lambda'\lambda > 0$.*

c.) *If $\alpha > 0$, then* $\operatorname{tr}(\alpha) > 0$.

Proof. Our statements are immediate from Proposition 1 and the definitions.

As a corollary to Theorem 2, we shall see that if $\alpha > 0$ and $\lambda'\alpha \neq 0$, then actually $\lambda'\alpha\lambda > 0$.

We shall give below some equivalent conditions for an endomorphism to be positive. Referring to Albert [1] and Morikawa [5] we recall first an abstract theorem for the convenience of the reader.

THEOREM 2. *Let R be an algebra over the rationals $\boldsymbol{Q}$, with an involution $x \to x'$ satisfying $(xy)' = y'x'$ and $(x')' = x$, and a $\boldsymbol{Q}$-linear functional $\sigma \colon R \to \boldsymbol{Q}$ which satisfies $\sigma(xy) = \sigma(yx)$, and such that for $x \neq 0$ we have $\sigma(xx') > 0$. Then:*

1.) *R is semisimple.*

2.) *If $x = x' \neq 0$, then $\boldsymbol{Q}[x]$ is a direct sum of totally real fields.*

3.) *If $x = x' \neq 0$, then $\sigma(yxy) \geqq 0$ for all $y \in \boldsymbol{Q}[x]$ if and only if x is a sum of squares in $\boldsymbol{Q}[x]$.*

Proof of 1. We first prove that if $x = x' \neq 0$, then x cannot be nilpotent. If it were, then we would have $x^{2^m} = 0$ but $x^{2^{m-1}} \neq 0$, and hence $x^{2^m} = (x^{2^{m-1}})^2 = 0$. As $x^{2^{m-1}}$ is symmetric, this contradicts the strict positivity of σ. Now if $x \neq 0$ is an element of a nilpotent right ideal, then xx' is symmetric, is in the ideal, and hence is nilpotent, thereby contradicting again the positivity of σ.

Proof of 2. Consider $\boldsymbol{Q}[x]$ with $x = x' \neq 0$. It is a commutative subalgebra of R, and the involution and trace on R induce on it an involution and trace with similar properties. Being semisimple, it is a direct sum of fields. On each such field F we have again induced an involution and a trace. We may therefore assume that $R = F$. But any $\boldsymbol{Q}$-linear function on F is of type $\sigma(\xi) = S(\alpha\xi)$ for some α in F. Here S denotes the ordinary trace from F to $\boldsymbol{Q}$. We have by assumption $S(\alpha\xi^2) = \sigma(\xi^2) > 0$, if $\xi \neq 0$. If some conjugate of α is not real, then the corresponding conjugate of F is dense in the complex numbers, and we choose $\xi \in F$ such that $\alpha\xi^2$ is very large negative at this conjugate, and very close to 0 everywhere else. This gives a contradiction, and α is totally positive. Similarly, one sees that R is totally real.

Proof of 3. We may again assume that $R=F$ is a totally real field. Then $\sigma(x\xi^2)>0$ for all $x\neq 0$ in F, and as we have seen above, this implies that x is totally positive. Hence it is a sum of squares. The converse is equally clear. This concludes the proof of our theorem.

COROLLARY 1. *Let R me as in the theorem, and $\xi\in R$ be such that $\xi=\xi'$, and $\sigma(\lambda\xi\lambda)\geqq 0$ for all $\lambda\in \boldsymbol{Q}[\xi]$. Then given $\beta\in R$ such that $\beta'\xi\beta\neq 0$, we have $\sigma(\beta'\xi\beta)>0$.*

Proof. We can write $\xi=\sum y_i^2$ with $y_i\in\boldsymbol{Q}[\xi]$. If we put $\mu_i=y_i\beta$, then at least one element $\mu_i'\mu_i$ is not 0, and

$$\sigma(\beta'\xi\beta)=\sum\sigma(\mu_i'\mu_i)>0.$$

COROLLARY 2. *Let R be as in the theorem, let $\alpha=\alpha'$ and assume that α is a sum of squares in $\boldsymbol{Q}[\alpha]$. If $\lambda\in R$ and if $\lambda'\alpha\neq 0$, then $\lambda'\alpha\lambda\neq 0$.*

Proof. Writing $\alpha=\sum\beta_i^2$ with $\beta_i\in\boldsymbol{Q}[\alpha]$, we must have $\lambda'\beta_i\neq 0$ for some i. Hence $0\neq(\lambda'\beta_i)(\lambda'\beta_i)'=\lambda'\beta_i^2\lambda$. Since $\sigma(\lambda'\beta_i^2\lambda)\geqq 0$ for each i, and for at least one i is >0, this shows that $\lambda'\alpha\lambda$ cannot be 0.

THEOREM 3. *Let $\alpha\in H_{\boldsymbol{Q}}(A)$ and assume $\alpha=\alpha'\neq 0$. Then the following conditions are equivalent:*

1.) *α is positive.*

2.) *All the characteristic roots of α are totally real and totally positive.*

3.) *α is a sum of squares in $\boldsymbol{Q}[\alpha]$.*

Proof. The equivalence between 2.) and 3.) is well known. If α is positive, and $\beta\in\boldsymbol{Q}[\alpha]$ then by D10 and the definition of the trace, we see that $\operatorname{tr}(\beta\alpha\beta)\geqq 0$. Hence α is a sum of squares by Theorem 2. This proves that the first condition implies the third. If we can write $\alpha=\sum\beta_i\beta_i'=\sum\beta_i^2$ with $\beta_i\in\boldsymbol{Q}[\alpha]$, then there is an integer $e>0$ and there are positive divisors Y_i such that $(e\beta_i)(e\beta_i)'=\varphi_X{}^{-1}\varphi_{Y_i}$ (Proposition 1). Putting $Y=\sum Y_i$, we see that $e^2\alpha=\varphi_X{}^{-1}\varphi_Y$, and hence that α is positive.

COROLLARY 1. *If α and β are two symmetric elements of $H_{\boldsymbol{Q}}(A)$ such that $\alpha>0$, $\beta>0$ and $\alpha\beta\neq 0$, then $\operatorname{tr}(\alpha\beta)>0$.*

Proof. We write $\alpha=\sum\lambda_i^2$ with $\lambda_i\in\boldsymbol{Q}[\alpha]$, and we have therefore $\operatorname{tr}(\alpha\beta)=\sum\operatorname{tr}(\lambda_i^2\beta)=\sum\operatorname{tr}(\lambda_i\beta\lambda_i)\geqq 0$. Actually, for some i, we have

$\lambda_i\beta \neq 0$, and hence by Corollary 2 of Theorem 2, $\lambda_i\beta\lambda_i \neq 0$. Hence the strict inequality holds, as desired.

COROLLARY 2. *Let* $Y > 0$ *be a divisor on* A, *and* $Z^* > 0$ *a divisor on* $\hat{A}$. *If* $\alpha = \theta^{-1}\varphi_{Z^*}\varphi_Y$ *and* $\alpha \neq 0$, *then* $\operatorname{tr}(\alpha) > 0$.

Proof. Let $\lambda = \varphi_X^{-1}\varphi_W$ with $W = \varphi_X^{-1}(Z^*)$ and let $\beta = \varphi_X^{-1}\varphi_Y$. We use the commutativity relations (3) and (4) to conclude that $\alpha = \lambda\beta$, and we can then apply Corollary 1.

Finally, note that if the abelian variety is defined over a finite field k with q elements, if X is rational over k, and if π is the Frobenius endomorphism, then from the relation $\pi\pi' = q\delta$, we can conclude from the above considerations without taking powers of π that the characteristic roots have absolute value $q^{\frac{1}{2}}$. Indeed, the algebra generated over $\boldsymbol{Q}$ by π and π' is commutative, and, in view of Theorem 2, is a direct sum of fields which are either totally real, or totally imaginary such that $x \rightarrow x'$ is the complex conjugation. If e_i is the idempotent of one of those fields, and if we put $\pi_i = \pi e_i$, then we see directly that the absolute value of π_i is $q^{\frac{1}{2}}$.

Appendix.

We shall now reproduce Weil's proof that if X is a divisor, $X \equiv 0$, then X is numerically equivalent to 0. The only property of abelian varieties that is used is the theorem of the square. To begin with, we have:

THEOREM. *Let* $f\colon C \rightarrow A$ *be a rational map of a complete non-singular curve into* A, *such that* $f(C)$ *generates* A (i.e., $A = f(C) + \cdots + f(C)$ *n times, where* $n = \dim A$). *Let* $W = \sum_{1}^{n-1} f(C)$. *Let* $X \equiv 0$ *be a divisor on* A, *and let*

$$f^{-1}(X) = \sum m_j(P_j).$$

(*If necessary, make a generic translation on* X *so that* $f^{-1}(X)$ *is defined.*) *Let* $M_1, \cdots, M_n$ *be independent generic points of* C *over a common field of definition* k *for* f, C, *and* A, *and let*

$$d = [k(M_1,\cdots,M_n) : k(\sum_{i=1}^{n} f(M_i))],\quad d_0 = [k(M_1,\cdots,M_{n-1}) : k(\sum_{i=1}^{n-1} f(M_i))].$$

Then $dX \sim nd_0 \sum m_j W_{f(P_j)}$.

Proof. Let $f_n\colon C \times \cdots \times C \rightarrow A \times \cdots \times A$ be the product of f with itself n times, and s_n the sum on A. Let $F = s_n f_n$. Then d is the degree of F. A standard computation yields $F\circ F^{-1}(X)=dX$. On the other hand, using step 1 in Theorem 1, we get

$$F^{-1}(X)\sim\sum_i f_n^{-1}p_i^{-1}(X),\ \text{which is}\ \sum_j m_j\sum_{i=1}^{n}(C\times\cdots\times P_j\times\cdots\times C).$$

We shall take F of this, and see that it gives the desired result. Let G be the graph of F, and let P be a generic point of C. Then by F-VII$_6$ Th. 12, we first take $G(P)$ on the product $C\times\cdots\times\hat{C}\times\cdots\times C\times A$ (where C is omitted in the i-th place), i. e., we take the projection on this variety of

$$G\cdot(C\times\cdots\times P\times\cdots\times C\times A).$$

This is a variety, whose set theoretic projection on A is $W_{f(P)}$. Taking now its projection on A in the sense of intersection theory, we obviously get $d_0W_{f(P)}$. If we work with a special point P_j which is a specialization of P, then we use the compatibility of intersection and projection with specializations, together with the fact that $W_{f(P)}$ has the uniquely determined specialization $W_{f(P_j)}$, to conclude the proof.

Now by the theorem of the square, we get

$$nd_0\sum m_j(W_{f(P_j)}-W)\sim W_u-W\equiv 0,$$

where $u=nd_0\sum m_jf(P_j)$. Consequently, we get $0\equiv dX\equiv nd_0(\sum m_j)W$. If we can prove that $\sum m_j=0$, this will show immediately that $dX\sim W_u-W$ and will prove the numerical equivalence of X to 0. We are therefore reduced to proving the following lemma.

LEMMA. *Let Y be a divisor, $Y>0$. Then Y cannot be $\equiv 0$.*

Proof. If $Y\equiv 0$, then for t generic on A, we have $Y_t\sim Y$. This would yield a representation of A into the complete linear system of Y, and thus a representation of A into the projective linear group. This representation must be trivial, and hence $Y_t=Y$, which is an absurdity.

It should be noted that Morikawa's Lemma 7 [5] is an immediate consequence of the above result, which, in fact, shows that the divisor W is non-degenerate. Cf. also Weil's arguments concerning the projective embedding of abelian varieties [7].

COLUMBIA UNIVERSITY.

REFERENCES.

[1] A. Albert, "On involutorial algebras," *Proceedings of the National Academy of Sciences*, vol. 41 (1955), pp. 480-482.

[2] I. Barsotti, "Il teorema di dualita per le varieta abeliane ed altri risultati," *Rendiconti di Matematica e delle sue applicazioni*, vol. 13 (1954), pp. 1-17.

[3] W. L. Chow, "Abstract theory of the Picard and Albanese varieties," to appear.

[4] H. Hasse, "Über die Riemannsche Vermutung in Funktionenkörpern," *Comptes Rendus du Congres International des Mathématiciens*, Oslo, 1936, pp. 189-206.

[5] H. Morikawa, "On abelian varieties," *Nagoya Mathematical Journal*, vol. 6 (1953), pp. 151-170.

[6] A. Weil, *Variétés abéliennes et courbes algébriques*, Hermann et Cie., Paris, 1948.

[7] ———, On the projective embedding of abelian varieties, in the volume in honor of S. Lefschetz, Princeton, 1957.

[8] ———, "On the theory of complex multiplication," *Proceedings of the International Symposium on Algebraic Number Theory*, Tokyo-Nikko. 1955. pp. 9-22.

SCHWARZ'S LEMMA AND A SINGULARITY OF BRIOT-BOUQUET.*

By Aurel Wintner.

---

1. The following lemma (in which

$$(1) \qquad f(z,w) = \sum_{m+n>0} c_{mn} z^m w^n \equiv \sum_{i=1}^{\infty} f_i(z,w), \text{ where } f_i = \sum_{m+n=i},$$

need not be divisible by z) contains (if (1) is chosen to be divisible by z) the classical result on the initial-value problem

$$(2) \qquad w' = g(z,w), \qquad w(z)\,|_{z=0} = 0, \qquad (w' = dw/dz),$$

where g $(\equiv f/z)$ is a function regular at $(z,w) = (0,0)$.

Lemma. *Let a function $f(z,w)$ of two complex variables be regular on the dicylinder*

$$(3) \qquad |z| < 1, \qquad |w| < 1,$$

and let

$$(4) \qquad |f(z,w)| \leqq 1 \text{ on } (3)$$

and

$$(5) \qquad f(0,0) = 0$$

[*hence*

$$(4\,\text{bis}) \qquad |f(z,w)| < 1 \text{ on } (3)].$$

Then the (singular) initial-value problem

$$(6) \qquad zw' = f(z,w), \qquad w\,|_{z=0} = 0$$

has a unique solution $w = w(z)$ which is regular on the circle

$$(7) \qquad |z| < 1.$$

It will be clear from the proof how this lemma can be worded so as to apply when the single equation (6) is replaced by a system, that is, when the w and the f of (6) are vectors.

---

* Received June 16, 1957.

2. Since (1) holds on (3), it follows from (4) that $|c_{mn}| \leqq 1$ (Cauchy), where sign of equality holds only if $f(z,w)$ is $w^m z^n$ times a constant of absolute value 1. In particular

$$|c_{01}| < 1 \tag{8}$$

unless (6) reduces to

$$zw' = cw, \qquad w|_{z=0} = 0, \qquad (|c| \neq 1), \tag{8 bis}$$

and (8 bis) is trivial, since its only solution is $w(z) \equiv 0$. But (8) is certainly sufficient for

$$c_{01} \neq 1, 2, \cdots, \tag{9}$$

the "eigenvalue" condition of Briot and Bouquet, who have shown that, under the proviso (9), there must exist for (6) a unique regular solution $w(z)$ on *some* circle $|z| <$ const., in which, however, the "sufficiently small" value of the const. remains unspecified* (correspondingly, neither (3) nor (4), but merely the absolute convergence of (1) on *some* neighborhood of $(z,w) = (0,0)$ is needed in this result).

Accordingly, the point in the lemma is the specification of the radius of regularity for $w(z)$, that is, the assertion that, under the assumption (4) for (1), the entire circle (7), admitted in (3) for $f(z,w)$, follows for $w(z)$.

3. Actually, the interest of the lemma lies in a final nature of the (normalized) absolute constants which it supplies.

First, if (4) is relaxed to the assumption that

$$|f(z,w)| < 1 + \epsilon \text{ on } (3), \qquad (\epsilon > 0), \tag{4*}$$

where $\epsilon > 0$, while all the other assumptions of the lemma are satisfied, then, no matter how small the positive constant ϵ may be, (6) need not have a solution $w(z)$ which is regular on (7). As a matter of fact, (6) *need not have any solution* $w(z)$ (*regular at* $z=0$) *if* (4) *is replaced by* (4*). This is shown by the example $f(z,w)=\epsilon z+w$, which satisfies (4*) but reduces the first of the equations (6) to $dw/dz=\epsilon+w/z$, a linear differential equation for which every solution $w=w(z)$ becomes singular at $z=0$ if $\epsilon=\text{const.}\neq 0$.

---

* For three variants of the proof of Briot and Bouquet, see, respectively, L. Schlesinger, *Einführung in die Theorie der Differentialgleichungen* (1900), pp. 103-107; E. L. Ince, *Ordinary differential equations* (1926), pp. 295-296; L. Bieberbach, *Theorie der gewöhnlichen Differentialgleichungen* (1953), pp. 68-69. The circle $|z| <$ const., which results in this manner as an assured domain of regularity for $w(z)$, is very unsatisfactory. In fact, the procedures are such as to involve not only the prinicple of majorants but, what is worse, an appeal to the *calcul des limites* as well as an application of the local existence theorem of implicit functions (for the majorant). For a discussion of these matters in the regular case, cf. A. Wintner, Acta Math., vol. 96 (1956), pp. 142-156, and Rend. Palermo, ser. 2, vol. 5 (1957), pp. 275-287. The nature of the "best absolute constants" in the general case of (9) remains undecided.

Secondly, if all assumptions of the lemma are satisfied, then the radius ($=1$) of the circle (7) is the best absolute constant. What is more, $w(z)$ can become singular on the boundary of (7). In order to see this, choose $f(z,w)$ to be independent of w, say $f=f(z)$, and put $g(z)=f(z)/z$. Then (4) and (5) will be satisfied if $g(z)$ is regular on (7) and $|g(z)|<1$ holds on (7). Since this is compatible with a function $g(z)$ having the circumference $|z|=1$ as a natural boundary, and since (6) now requires that $w(z)=\int g(z)dz$ (with $w(0)=0$), the assertion follows.

Remark. The *formal* source of all of this is the circumstance that $z\cdot(\ )'=zd(\ )/dz$ on the left of (6) as a *homogeneous operator, of degree* 0, *in* z. Let this operator be replaced by the *identity operator.* Then (6) becomes replaced by

$$w=f(z,w),\qquad w\,|_{z=0}=0. \tag{6 bis}$$

And there results a correct statement *if* (6 bis) *is read, in place of* (6), *in the lemma of* § 1 (and if all the other assumptions, and the assertion, of the lemma are retained). This variant of the lemma, a theorem concerning implicit functions (rather than singular diffeerntial equations) is of a standard type. It can be proved, for instance, along the lines of Rouché's theorem, by appealing to general fixed point theorems (Poincaré-Brouwer).

Another proof for the case (6 bis) follows directly along the lines of the proof to be given for the case (6). But the resulting approach to (6 bis) is more straightforward (cf. § 11), since it does not involve, as (6) does, a Schwarzian lemma (cf. § 4). This contrast makes sufficiently clear the actual content of the lemma of § 1.

4. The proof of the italicized statement of § 1 will substantially depend on the following corollary of Schwarz's lemma (which explains the title of this paper):

Let $g(z)$ *be a function which is regular for* $|z|<1$, *vanishes at* $z=0$, *and satisfies the inequality* $|g(z)| < 1$ *for* $|z| < 1$. *Let* $w = w(z)$, *where* $|z| < 1$, *denote the* (*unique, regular*) *solution of the initial-value problem*

$$zw' = g(z), \qquad w|_{z=0} = 0. \tag{10}$$

Then $|w(z)| < 1$ *for* $|z| < 1$.

In fact, if $h(z) = g(z)/z$, then $|h(z)| < 1$ for $|z| < 1$. But (10) means that

$$w(z) = \int_0^z h(\zeta)\,d\zeta; \text{ hence } |w(z)| \leqq \int_0^{|z|} |d\zeta|,$$

and so $|w(z)| \geqq |z|$, where $|z| < 1$.*

5. This Schwarzian lemma will now be combined with the process of successive approximation, which will be set up as follows:

$$zw_{k+1}'(z) = f(z, w_k(z)), \qquad w_{k+1}(0) = 0, \tag{11}$$

where $w_0(z)$ is any function which is regular on (7) and satisfies the case $k = 0$ of the following pair of conditions:

$$|w_k(z)| < 1 \text{ on } (7), \text{ and } w_k(0) = 0 \tag{12}$$

(for instance, $w_0(z) \equiv 0$).

Suppose that, for a fixed $k \geqq 0$, the function $w_k(z)$ has been defined on (7) so as to be regular and to satisfy (12). Then, since $f(z, w)$ is regular on (3) and satisfies (4) and (5), the function $g_k(z) = f(z, w_k(z))$ is regular on (7), satisfies $|g_k(z)| < 1$ on (7), and $g_k(0) = 0$. Hence, if (11) is identified with (10), it follows from the lemma of § 4 that $w_{k+1}(z)$ is regular on (7) and satisfies $|w_{k+1}(z)| < 1$ on (7). This completes the induction.

6. It will be shown in § 7 that the sequence

$$w_1(z), \cdots, w_k(z), \cdots, \quad \text{where } w_k(0) = 0, \tag{13}$$

is convergent on a certain circle

$$|z| < d, \qquad\qquad (d \leqq 1), \tag{14}$$

---

* The *best* estimate of $|w'(z)|$ for *fixed* z and *variable* g in (10) is supplied by a substantially deeper result of Dieudonné (depending on Pick's non-euclidean formulation of Schwarz's lemma; cf. p. 18 of Carathéodory's *Funktionentheorie*, vol. 2, 1950) which, however, does not lead to $|w(z)| < 1$ on $|z| < 1$ for *fixed* g.

for which the value of d will not be determined. But since the functions (13) are regular on (7) and satisfy (12), it will follow from the oldest theorem (Stieltjes) of the theory of normal families that the sequence (13), being convergent on (14), must be uniformly convergent on every closed subset of (7).

Let $w(z)$ be the limit function of (13) on (7). Then $w(z)$ is regular on (7) and is a solution of (6). This follows from the uniformity of the convergence if (11) is written in the form

$$(15) \qquad w_{k+1}(z) = \int_0^z f(\zeta, w_k(\zeta))/\zeta \, d\zeta, \qquad (|z| < 1).$$

In fact, it is clear from (4), (5) and (12) that, in view of Schwarz's lemma, the integrand of (15) is regular and (in k) uniformly bounded on (7).

7. The proof of the convergence of (13) on (14) (if d is small enough) proceeds as follows:

Let (1) be written in the form

$$(16) \qquad f(z,w) = c_{10}z + c_{01}w + h(z,w), \text{ where } h(z,w) = \sum_{i=2}^{\infty} f_i(z,w).$$

Then $h(z,w)$ is regular on (3) and contains only terms of second or higher order (in z and w together), which implies that $\partial h/\partial w \rightarrow 0$ as $(z,w) \rightarrow (0,0)$. Hence it is clear that there belongs to every $\epsilon > 0$ a pair of positive numbers, say $d = d_\epsilon$ and $D = D_\epsilon$, which are less than 1 and have the property that the absolute value of the difference $h(z,w^*) - h(z,w^{**})$ will not exceed $\epsilon \, | w^* - w^{**} |$ whenever z, w^*, w^{**} are complex numbers within the respective circles $|z| < d$, $|w^*| < D$, $|w^{**}| < D$. On the other hand, it is seen from (12) and from Schwarz's lemma that, if $D = D_\epsilon$ is fixed and $d = d_\epsilon$ is chosen small enough, then $|w_k(z)| < D$ will hold on (14) for every k. Consequently,

$$(17) \qquad |h(z, w_k(z)) - h(z, w_{k-1}(z))| \leqq \epsilon \, |w_k(z) - w_{k-1}(z)| \text{ on } (14),$$

where ϵ and $d = d_\epsilon$ are independent of k.

According to (11), (16) and (17),

$$(18) \qquad |zw_{k+1}'(z) - zw_k'(z)| \leqq 0 + (|c_{01}| + \epsilon) |w_k(z) - w_{k-1}(z)| \text{ on } (14).$$

But if the trivial case (8 bis) is disregarded, then (8) holds and so, if the postitive number ϵ (which thus far was arbitrary) is chosen small enough, the sum $|c_{01}| + \epsilon$ will be less than 1. Consequently, from (18),

$$(19) \qquad |zu_{k+1}'(z)| \leqq \theta \, |u_k(z)| \text{ on } (14),$$

where $\theta = \text{const.} < 1$ and

$$u_k(z) = w_k(z) - w_{k-1}(z). \tag{20}$$

Finally, it is clear from (12) and from Schwarz's lemma that, if d is chosen small enough, the functions (20) will be such as to satisfy $|u_k(z)| < 1$ on (14) (in fact, $d < \frac{1}{2}$ is sufficient to this end). In addition, $u_k(0) = 0$, since $w_k(0) = 0$. Hence, if Schwarz's lemma is applied to (19) in the same way as it was applied to (10) in the proof of the italicized assertion of § 4, it is seen, by induction, that (19) leads to

$$|u_k(z)| < \text{const.}\,\theta^k \text{ on } (14). \tag{21}$$

In fact, since the operator zd/dz remains invariant under the substitution $z \to Rz$, where R is a positive (or just non-vanishing) constant, it is clear that in contrast with Schwarz's own lemma, its "integral" corollary, that formulated in § 4, is independent of the radius of the z-circle (so that $|z| < 1$ can be replaced by any $|z| < d$).

8. Since the (positive) constant θ is less than 1, the convergence of the sequence (13) on the circle (14), chosen in § 7, is clear from (21) and (20). According to § 6, this proves that (6) has a solution $w(z)$ which is regular on the entire circle (7). Hence, in order to complete the proof of the lemma of § 1, all that remains to be ascertained is that (6) cannot have two distinct solutions (which are regular at $z = 0$).

The truth of this assertion of uniqueness is trivial in the case (8 bis). Hence it is sufficient to consider the case (8). But (8) implies (9) and, according to Briot and Bouquet, (9) alone is sufficient in order that the solution $w(z)$ of (6) be unique (in a neighborhood of $z = 0$).

The classical proof of this fact depends on a comparison of coefficients. Another proof (valid in the case (8) only) results by an adaptation of the "Lipschitz" uniqueness proof, customary in the real field. In fact, if $w = w(z)$ and $w = v(z)$ are regular solutions of (6) on (14), then it is clear from § 7 that, corresponding to (19) and (20),

$$|zu'(z)| \leqq \theta\,|u(z)|, \text{ where } u(z) = w(z) - v(z) \tag{22}$$

and $\theta < 1$, holds on (14), if d is small enough. But (22) leads to what results if $u_k(z)$ is replaced by $u(z) = w(z) - v(z)$ in (21), which means that $w(z) \equiv v(z)$ holds (on (14) and, therefore, on (7)).

9. The italicized assertion of § 1 can be completed by the following facts:

Under the assumption of the Lemma of § 1,

(i) *both*

$$|w(z)| < 1 \text{ and } |w'(z)| \leqq 1, \text{ where } |z| < 1, \tag{23}$$

hold for the solution of (6) (*and the sign of equality is excluded in* (23) *unless* (1) *is of the form* $f(z, w) = Cz$, *where* $|C| = 1$);

(ii) *if* c_{10} *and* c_{01} *are the coefficients of the linear terms in* (1), *then the solution* $w(z)$ *vanishes identically unless* $|c_{01}| < 1$; *while if*

$$c_{01} \neq 1 \text{ and } c_{10} \neq 0, \tag{24}$$

then

$$w'(0) = a \neq 0, \text{ where } a = c_{10}/(1 - c_{01}) \tag{25}$$

(*so that* $w(z)$ *is schlicht near* $z = 0$);

(iii) *if* (24) *is satisfied, then the inverse,* $z = z(w)$, *of* $w = w(z)$, *where* $w(0) = 0$, *is schlicht, and less than* 1 *in absolute value, on the circle* $|w| < |a|^2$, *where* $a = c_{10}/(1 - c_{01})$.

If (i) and the second part of (ii) are granted, then (iii) follows if a result of Landau, which he obtained in connection with his treatment of the problem of Bloch's constant, is used in the same way as I used it recently (vol. 78 (1956), pp. 552-553, of this Journal) in the *regular* case, (2), of (6). In fact, it is sufficient to combine (23), (24) and (25) with theorem (*) on p. 552, loc. cit., in order to obtain (iii) (the proof of (*), depending on Landau's result, is on p. 553, loc. cit.). Accordingly, only (i) and (ii) remain to be proved.

10. It is clear from the process of sucessive approximations which led to $w(z)$ that $|w(z)| < 1$ for $|z| < 1$; cf. (3)-(7). Hence it is clear from (4) that the function $\phi(z) = f(z, w(z))$ is regular, and does not exceed 1 in absolute value, on the circle $|z| < 1$. In addition, $\phi(0) = 0$ and $w'(z) = \phi(z)/z$, by (5) and (6). It follows therefore from Schwarz's lemma that $|w'(z)| \leqq 1$ if $|z| < 1$, where the sign of equality is excluded unless $w(z) = Cz$, where $|C| = 1$.

This proves (i). Since the first part of (ii), that concerning the identical vanishing of $w(z)$, is contained in the remark made in connection with (8)-(8 bis), only the assertion of the second part of (ii) remains to be proved.

That assertion assumes (24) and claims (25). Hence it is sufficient to verify that, whether (24) is satisfied or not,

$$(1-c_{01})a = c_{10}. \tag{26}$$

But if (1) and $w(z) = w(0) + w'(0)z + \cdots$, where $w(0) = 0$ and $w'(0) = a$, are inserted in (6), then it is seen that

$$z(a + \text{const.}\, z + \cdots) = c_{10}z + c_{01}(az + \cdots) + \cdots,$$

where the dots are terms which are of second or higher order in z. Hence (26) is obvious.

11. It is easy to see how the theorem mentioned in the Remark of § 3 can be proved by the method applied above. The assertion of that theorem is that the implicit equation $w = f(z, w)$ possesses a unique solution $w = w(z)$, satisfying $w(0) = 0$, which is regular (and less than 1 in absolute value) on the entire circle $|z| < 1$, if $f(z, w)$ is regular on the dicylinder (3) and satisfies both (4) and (5).†

---

† In the particular case in which $f(z, w)$ is independent of z (so that (6 bis) reduces to $w = zf(w)$), this fact has the following variant: *If $f(w)$ is regular, and $|f(w)/w|$ is not less than a positive constant K, on the circle $|w| < 1$, and if $f = 0$ and $df/dw = 0$ at $w = 0$ (hence $K \geqq 1$), then the solution $w = w(z)$ of Lagrange's equation $w = zf(w)$ is a regular and schlicht function not exceeding* 1 *on the circle $|z| < \Omega(1/K)$, where*

$$\Omega(M) = (1 - \sqrt{(1 - M^{-2})})^2 M^3 \qquad (0 < M \leqq 1,\ \Omega(1) = 1)$$

(*and $\Omega(1/K)$ is the best absolute constant for every fixed K*). In order to see this, it is sufficient to put $F(w) = w/f(w)$, then to interchange the parts played by the variables z and w, and finally to apply the following theorem of Landau (quoted, after the correction of a misprint in the third line of the wording of the theorem on p. 91, from Valiron's *Fonctions Analytiques* (Paris, 1954), pp. 90-93): If a function $F(z)$ is regular, and does not exceed M in absolute value, on the circle $|z| < 1$, and if $F(0) = 0$ and $F'(0) = 1$ (hence, $0 < M \leqq 1$), then the local inverse, $z = \phi(w)$, of $w = F(z)$ is regular, and less than 1 in absolute value, on the circle $|w| < \Omega(M)$, and $\Omega(M)$ is the best absolute constant for every fixed M.

Correspondingly, if the preceding device of replacing z, w, f, K by $w, z, F, M = 1/K$ is used in the *reverse direction*, it is easy to verify that a result of Hartman and myself (Rend. Palermo, ser. 2, vol. 3 (1954), pp. 287-291) can simply be interpreted so as to state the following: *If $w = F(z)$, where $F(0) = 0$, is a regular function satisfying $|F(z)| \geqq |z|$ for $|z| < 1$, then the circle $|z| < 1$ is the (schlicht) image of a* convex *w-domain contained in the circle $|w| < 1$* (and containing, of course, the point $w = 0$). The wording of this curious assertion becomes understandable only if it is noted that, as readily seen from Rouché's theorem, the whole of the circle $|w| < 1$ must be contained in the w-image of the circle $|z| < 1$ (an image which is *schlicht* by necessity), if $w = F(z)$, where $F(0) = 0$, is a regular function satisfying $|F(z)| \geqq |z|$ for $|z| < 1$.

First, (4) and (5) imply that $|f(z,w)| < 1$ on (3), and so it follows from (1) that (8) holds unless $f(z,w)$ is of the form $c_{01}w$ (where $|c_{01}| = 1$). But the latter case can be disregarded, since it leads to the trivial solution $w(z) \equiv 0$. On the other hand, (8) means, by (1), that the absolute value of the partial derivative $f_w(z,w)$ is less than 1 at the point $(z,w) = (0,0)$, and so the partial derivative $(w - f)_w = 1 - f_w$ does not vanish there. Consequently, there exists a solution $w(z)$ on *some* circle $|z| < \epsilon$. But on such a circle, $w(z)$ can be obtained by the method of successive approximations also. For, in view of (8), there is available for (1) a uniform Lipschitz constant $\theta < 1$ on a sufficiently small dicylinder about the origin. The replacement of $|z| < \epsilon$ by $|z| < 1$ now follows, as above, by having recourse to Stieltjes' theorem on normal families.

12. Under appropriate restrictions on the terms actually occurring in (1), Briot and Bouquet and their successors[*] have dealt with the (local)

---

[*] For references, cf. p. 38 and p. 40 of Painlevé's article II, 15 in the *Enc. des Sci. Math.* (1910). In view of the comments which follow above, it is necessary to correct a curious oversight which runs through the literature initiated by pp. 95-100 of Borel's celebrated paper on divergent series (*Ann. Ec. Norm.*, ser. 3, vol. 16, 1899). There Borel proved for the case $N < \infty$ (of any polynomial not containing linear terms), and surmised for the case $N \leqq \infty$ (of any power series not containing linear terms; an extension subsequently proved, along the lines of Borel's treatment of the polynomial case $N < \infty$, by Rémoundos (1908); cf. footnote 124) in Painlevé's article, p. 38), that, if the differential equation is

$$z^2 w' = bw + \sum_{i=2}^{N} f_i(z,w), \qquad (2 \leqq N \leqq \infty), \tag{27 bis}$$

where $f_i(z,w)$ is, as in (1) and (27) above, a form of degree i, and b is a negative constant (so that $f_1(z,w)$ certainly does *not* vanish identically), then the situation is as follows: Not only can the coefficients a_k of the formal solution $w(z) = a_2 z^2 + \cdots$ of (27 bis) be calculated uniquely (Briot-Bouquet), but the Borel associate,

$$W(z) = \sum_{k=2}^{\infty} a_k z^k / k!, \text{ of } w(z) = \sum_{k=2}^{\infty} a_k z^k$$

will have a non-vanishing radius of convergence (which means that $| a_k / k! |^{1/k} = O(1)$, i.e., $| a_k |^{1/k} = O(k)$; this cannot be improved to $| a_k |^{1/k} = O(1)$, since $w(z)$ itself need not have a convergence circle). But in both editions of his *Leçons sur les séries divergentes* (p. 117 of the first edition (1901), p. 150 of the second edition (1928)), Borel misquotes his result, by claiming it simply for

$$z^2 w' = \sum_{k=2}^{N} f_k(z,w), \tag{27_0 bis}$$

rather than only for (27 bis), where $0 > b \neq 0$ (or, at least, $\operatorname{Re} b < 0$). Actually, even if the formal existence of the power series $w(z)$ is granted in the case (27_0 bis), the proof for the convergence of the associated power $W(z)$ (for small $|z| > 0$) breaks down completely, since $0 < -1/b < \infty$ (or, at least, $0 > \operatorname{Re}(-1/b) < \infty$) is essential problem which results if the differential operator zd/dz of the (non-local) lemma of § 1 is replaced, not by the identity operator of § 11 (which is again of degree 0), but by the differential operator z^2d/dz (of a positive degree); so that (6) becomes replaced by

$$(27) \qquad z^2w' = f(z, w), \qquad w\,|_{z=0} = 0, \qquad w'\,|_{z=0} = 0,$$

where, as before, $f(z, w)$ is a function regular in a neighborhood of the point $(0, 0)$ and vanishing at $(0, 0)$. Suppose that not only $f_0(z, w) \equiv f(0, 0) = 0$ but also $f_1(z, w) \equiv 0$ holds in (1) (this seems to be, but actually is not, the case in the literature initiated by Borel; cf. the preceding footnote). Then, with the exception of one point, the proof of the lemma of § 1 on (6) can be repeated. But that point, though only of a local nature, happens to be fundamental enough to vitiate the final result.

The same holds if the case $f_1(z, w) \equiv 0$ of (1) and (27) is generalized from $j = 2$ to any integer $j > 1$, as follows:

$$(28a) \qquad z^jw' = f(z, w), \qquad\qquad (28b) \qquad f(z, w) = \sum_{i=j}^{\infty} f_i(z, w),$$

where $f_i(z, w)$ is a form of degree i, as in (1). If $j = 1$, then (28a)-(28b) reduces to the differential equation of (6), since (5) was assumed in (6). Correspondingly, suppose that a function (28b), belonging to a given $j > 1$, is regular on the dicylinder (3) and satisfies (4).

Since $f_i(z, w) \equiv 0$ in (28 bis) if $i < j$, it is easily realized that, after j applications of Schwarz's lemma, the italicized lemma of § 4 can be extended (from $j = 1$ to any j) so as to lead to the following result: Corresponding to (11)-(13), where $j = 1$, the $1 + j$ conditions

$$(11_j) \qquad z^jDw_k(z) = f(z, w_{k-1}(z)); \qquad D^hw_k(0) = 0, \qquad 0 \leqq h < j,$$

where $w_0(z) \equiv 0$ and $D = d/dz$ (with $D^h = DD^{h-1}$ and $D^0v = v$), define for every k (> 0) a unique function $w_k(z)$ which is regular on (7) and satisfies the j inequalities

$$(12_j) \qquad |D^hw_k(z)| < 1 \text{ on } (7), \text{ where } 0 \leqq h < j$$

(in particular, (12) holds). Hence, the argument applied in the case $j = 1$ could be repeated without any change if the purely *local* aspect of the issue were in order, namely, if the sequence $w_1(z), w_2(z), \cdots$ of the successive

---

indeed in the majorization process on which the proof depends in the case (27 bis). Curiously enough, the error is repeated in the report of Painlevé (p. 38, loc. cit., is so explicit as to say that *b peut être nul*), who must have been misled both by Borel's and Rémoundos' mistaken formulations of what they had actually proved.

approximations, just secured on (7), were convergent on *some* circle $|z| < \epsilon$, as in § 7.

But precisely this classical (local) part of the issue leads to difficulties if the fixed j is greater than 1 in the initial value problem which, for a function $w(z)$ in a neighborhood of $z = 0$, is assigned by

$$(28c) \qquad D^h w(0) = 0, \qquad 0 \leqq h < j,$$

and (28a), with (28b). Apparently, the difficulties cannot be overcome without placing very specific restriction (to be supplied by a Newton polygon) on the set of the $j+1$ coefficients a_{mn} of the leading term,

$$(1_j) \qquad f_j(z, w) = \sum_{m+n=j} c_{mn} z^m w^n, \qquad (f_j \not\equiv 0),$$

of the double power series (28b). [Correspondingly, it is possible to allow in the power series (1) of (28a) a leading term $f_i(z, w)$ having a degree $i = i_0$ lower than the exponent j on the left of (28a), provided that still more specific restrictions are placed on the $i_0 + 1$ coefficients c_{mn} of that leading term.]

Appendix I.

If the function $g(z, w)$ occurring in (2), § 1, is now denoted by $f(z, w)$, then the classical result of the successive approximations, the result referred to at the beginning of § 1, is as follows:

(i) *If* $f(z, w)$ *is regular on the dicylinder*

$$(1) \qquad (|z| < 1, |w| < 1)$$

and if $f(z, w)$ *is bounded,*

$$(2) \qquad |f(z, w)| \leqq M \text{ on } (1),$$

then the solution $w = w(z)$ *of the initial-value problem*

$$(3) \qquad dw/dz = f(z, w), \qquad w|_{z=0} = 0$$

exists, as a regular function satisfying

$$(4) \qquad |w(z)| < 1,$$

on the circle

$$(5) \qquad |z| < \min(1, M^{-1})$$

(*at least*). With regard to the last (parenthetical) remark, it is known that the radius of the circle (5) is the best *absolute* constant for every fixed value of the positive constant M occurring in (2); cf. my note in vol. 57 (1935), pp. 539-540, of this Journal.

Whereas the assumption (2) of (i) represent an *upper* limitation, (i) has a curious counterpart, (ii) below, in which only a *lower* limitation, $|f(z,w)| \geqq K = \text{const.} > 0$, is assumed. But it will be clear from the proof that K cannot be allowed to be less than 1; so that, in view of the comments made in the first part of § 3, the resulting dual of (i) lies along the lines of the Lemma (§ 1), rather than of (i) itself. The dual of (i) in question, which I considered in a rough form (and, in addition, in terms of a normalization which disguises the true situation) on pp. 551-553 of vol. 78 (1956) of this Journal, is as follows:

(ii) *Let* $f(z,w)$ *be regular on* (1) *and, on* (1), *let* $|f(z,w)|$ *be bounded from below by a constant which is not less than* 1 (*i.e., let*

$$(6) \qquad K \geqq 1, \text{ and } |f(z,w)| \geqq K \text{ on } (1),$$

while (2) *need not hold for any* $M < \infty$). *Then the solution* $w = w(z)$ *of* (3) *exists, as a regular function satisfying* (4), *on the circle*

$$(7) \qquad |z| < \phi(\theta), \text{ where } \theta = K/|f(0,0)|$$

[*hence,* $0 < \theta \leqq 1$, *by* (6)], *if* $\phi = \phi(\theta)$ *denotes the* (*positive, increasing*) *function*

$$(8) \qquad \phi(\theta) = 1 - (1 - \theta^{-2}) \log(1 - \theta^2), \qquad (0 < \theta \leqq 1),$$

where $\phi(+0) = 0$, $\phi(1) = 1$.

Remark. It will be clear from the proof that *either the regular function element* $w = w(z)$, *given on the circle* (7), *or a direct analytic prolongation of this function element must attain, at some* $z = z(w)$, *every value* w *contained in the circle* $|w| < 1$. But this, together with the fact that (3) and (6) imply the non-vanishing of $dw(z)/dz$ (hence the *unramified* character of the inverse function) on (7), does not of course mean that $w(z)$ is *schlicht* on the circle (7).

The proof of (ii) will follow by an appropriate combination of two known facts, those listed under (I) and (II) below. The application of these two facts will be made possible by writing (3) in the form

$$(9) \qquad dz/dw = 1/f(z,w), \qquad z\,|_{w=0} = 0,$$

i.e., by first interchanging the parts played by z and w.

(I) The classical result (the result which supplies the radius of (5) if $a = 1$ and $b = 1$) states that if $f(z, w)$ is regular, and does not exceed M in absolute value, on a dicylinder $(|z| < a, |w| < b)$, then the solution $w = w(z)$ of (3) is regular, and satisfies the inequality $|w(z)| < b$, on the circle $|z| < \min(a, b/M)$.

(II) A theorem of Landau (his Satz X on p. 473 of his paper in the Sitzber. Preuss. Akad. Wiss., 1926) states that if a function $w = w(z)$ is regular, and has a derivative $w' = dw/dz$ satisfying the inequality $|w'(z)| \leqq S/R$, on the circle $|z| < R$, where R and S are given positive numbers, and if $w(0) = 0$ and $w'(0) \neq 0$, then the (local) inverse function, $z = z(w)$, of $w = w(z)$ (i.e., the function element $z(w)$ assigned, near $w = 0$, by $w(0) = 0$ or $z(0) = 0$) is regular, and less than R in absolute value, on the circle $|w| < S\phi(\theta)$, where θ and $\phi(\theta)$ are defined by $\theta = R\,|w'(0)|/S$ and (8) respectively (clearly, the assumption $0 < \theta \leqq 1$ of (8) is satisfied, and $\theta = 1$ holds only in the trivial case $f(z) = \text{const.}\, z$). Landau (loc. cit.) has also shown that the radius of his w-circle is the best absolute constant for any given triple of positive numbers $R, S, |w'(0)|$.

In order to prove (ii), suppose that $f(z, w)$ is regular on (1) and that there exists a constant K satisfying (6). Then, if z and w are interchanged, (3) becomes (9), and (I) is applicable when a, b, M and f are chosen to be 1, 1, K^{-1} and $1/f(z, w)$ respectively. Thus the radius of the w-circle supplied by (II) becomes $\min(1, K)$, which is 1, since $K \geqq 1$, by (6).

Accordingly, the solution $z = z(w)$ of (9) is regular, and satisfies the inequality $|z(w)| < 1$, on the circle $|w| < 1$. In addition, since $|1/f(z, w)| \leqq K^{-1}$ on (1), it follows from (9) that the absolute value of the derivative $dz(w)/dw$ does not exceed K^{-1} on the circle $|w| < 1$.

Consequently, if (II) is applied so as to interchange z and w, then the assumptions of (II) are satisfied when R, S and $|w'(0)|$ are chosen to be K, 1 and T respectively, where T denotes the value of $|dz(w)/dw|$ at $w = 0$. But (9) shows that $T = |f(0, 0)|^{-1}$, where $f(0, 0) \neq 0$, by (6). It follows therefore from (II) that the inverse function of $z = z(w)$, which is now the function $w = w(z)$, is regular, and satisfies the inequality $|w(z)| < 1$, on the circle (7). This proves (ii).

The question raised by the Remark, following (ii), can be answered if (II) is replaced by another theorem of Landau, which can be formulated as follows (cf., e.g., p. 95 of Valiron's *Fonctions Analytiques*, 1954):

(III) If $w(z)$ is regular, and satisfies the inequality $|w(z)| \leqq S$, on the circle $|z| < R$, and if $w(0) = 0$ and $w'(0) \neq 0$ (where $w' = dw/dz$), then $w(z)$ is *schlicht* on the circle $|z| < R\psi(\theta)$, where $\theta = R\,|w'(0)|/S$ (hence, $0 < \theta \leqq 1$), if $\psi = \psi(\theta)$ denotes the (positive, increasing) function

$$(10) \qquad \psi(\theta) = [1 - (1 - \theta^2)^{\frac{1}{2}}]/\theta \qquad (0 < \theta \leqq 1)$$

(so that $\psi(+0) = 0$, $\psi(1) = 1$). Landau also proved that the radius of his z-circle is the best absolute constant for any given triple of positive numbers R, S, $|w'(0)|$.

(ii bis) *Under the assumption of* (ii), *there exists a positive* $\lambda = \lambda(\theta)$, *depending only on the ratio* $\theta = K/|f(0,0)|$ *and having the property that the solution* $w = w(z)$ *of* (3) *is schlicht on the circle* $|z| < \lambda(\theta)$.

In fact, it is clear from (ii) and (III) that a $\lambda = \lambda(\theta)$ satisfying the requirements of (ii bis) can be obtained by composing the two positive functions (8), (10). No such composition is needed in what corresponds to (ii bis) when (ii) is replaced by the classical result (i):

(i bis) *If* $f(z,w)$ *is regular on* (1) *and satisfies* (2), *then the solution* $w = w(z)$ *of* (3) *fails to be schlicht on any circle* $|z| < \epsilon$ *if* $f(0,0) = 0$; *while if* $f(0,0) \neq 0$, *and if* $\psi(\theta)$ *is defined by* (10), *then* $w(z)$ *is regular and schlicht on the circle* $|z| < \psi(f(0,0)|)$ *or on the circle* $|z| < \psi(|f(0,0)|/M)/M$ *according as* $M \geqq 1$ *or* $M \leqq 1$.

In fact, $w'(0) = f(0,0)$, by (3). Hence the assertion of (i bis) is obvious for the case $f(0,0) = 0$. In the remaining case, it is seen from (i) that (III) is applicable with $S = 1$; $|w'(0)| = |f(0,0)| > 0$, and $R = 1$ or $R = M^{-1}$ according as $M \geqq 1$ or $M \leqq 1$. It is readily verified from (10) that, in both subcases of the case $f(0,0) \neq 0$, the z-circle supplied by (i bis) is contained in (and, except in the trivial case $|f(0,0)| = M$, where $f(z,w) = \text{const.}$, is *smaller* than) the z-circle, (5), of (i) itself.

* *
*

Let finally be mentioned the following theorem (ii_0) which, on the one hand, represents the limiting case of (ii) and, on the other hand, can be interpreted as a refined form of (the local part of) a classical result (Briot-Bouquet, Fuchs, Poincaré) on the exceptional standing of Riccati's equation:

(ii_0) *If the coefficients of a quadratic polynomial*

$$(11) \qquad f(z,w) = \alpha(z)w^2 + \beta(z)w + \gamma(z)$$

are regular and bounded on a circle $|z| < a$, *and if* b, L *is a pair of positive* *constants having the property that the absolute value of the quadratic polynomial* $\alpha(z) + \beta(z)w + \gamma(z)w^2$ *is less than* L *on the dicylinder* $(|z| < a, |w| < b)$, *then, unless* $\alpha(z)$ *vanishes identically, the (generalized Riccati) differential equation* $w' = f(z, w)$ *possesses on the circle*

$$(12) \qquad |z| < \min(a, (bL)^{-1})$$

a unique solution $w = w(z)$ *which is regular at every point* $z \neq 0$ *of the circle* (12) *and satisfies the "initial condition"* $w(0) = \infty$, *the function* $w(z)$ *having a pole at* $z = 0$; *in addition,* $|w(z)| > b$ *on* (12).

Note that $w' = f(z, w)$ is a Riccati equation of standard type, reducible by the substitution $w = v'/v$ to the linear differential equation $w'' + p(z)v' + q(z)v = 0$ (where $p = -\beta$, $q = -\gamma$), only if $\alpha(z)$ is identically 1; and that, even without regard to the explicit value of the radius* of the circle (12), division by $\alpha(z)$ introduces a singularity (of the linear differential equation of second order) at $z = 0$ if $\alpha(0) = 0$, whereas the vanishing of $\alpha(0)$ is allowed in (ii_0), the only restriction being the not *identical* vanishing of $\alpha(z)$, i.e., the exclusion of the linear case, $w' = \beta(z)w + \gamma(z)$, of $w' = f(z, w)$ itself.

In order to prove (ii_0), put $u = 1/w$, $F(z, u) = -u^2 f(z, 1/u)$, and $N = b^2 L$. Then (11) and the definitions of a, b, L show that $F(z, u)$ is regular, and less than N in absolute value, on the dicylinder $(|z| < b, |u| < b)$. Hence, $u' = F(z, u)$ has on the circle $|z| < \min(a, b/N)$ a unique (regular) solution $u = u(z)$ satisfying $u(0) = 0$, and $|u(z)| < b$ holds on this circle. Since the latter is precisely (12), the assertions of (ii_0) follow from $w(z) = 1/u(z)$. The exclusion of the identical vanishing of $\alpha(z)$ is needed in order to prevent that $w(z)$ becomes ∞ identically.

---

* For the case in which $\alpha(z)$ and $\beta(z)$ are identical with 1 and 0 respectively (so that $w' = f(z, w)$ reduces to $w' = \gamma(z) + w^2$), a radius sharper than that of (12) was obtained by Dieudonné (Bull. des Scien. Math., vol. 55 (1931), part 2, pp. 99-104), whose result is of a final nature in this case. His method, based on an adaptation of Sturm's comparison theorem to the complex field, contains *in nuce* what, in my papers referred to in the footnote to § 2 above, I called the "principle of subordination," and which goes back to a note of Nakano (Proc. Imp. Acad. Japan, vol. 8 (1932), pp. 29-31), a note of a somewhat later date than Dieudonné's paper dealing with $w' = \gamma(z) + w^2$. For an extension of Dieudonné's result to other Riccati equations (and for systems of such equations), cf. M. Müller, Math. Ztschr., vol. 41 (1936), pp. 174-175. Dieudonné's Sturmian inequality and the final nature of his absolute constant were rediscovered by Z. Nehari (Bull. Amer. Math. Soc., vol. 55 (1949), p. 549).

Appendix II.

The theorem of Briot and Bouquet, referred to in § 2, states that the differential equation

$$(1) \qquad zw' = az + \beta w + \phi(z,w), \text{ where } \phi(z,w) = \sum_{m+n \geqq 2} a_{mn} z^m w^n,$$

possesses on *some* circle about $z = 0$ a unique solution

$$(2) \qquad w(z) = \sum_{k=1}^{\infty} c_k z^k,$$

if the power series $\phi(z,w)$ converges on a neighborhood of $(z,w) = (0,0)$ and a, β are two constants the second of which is not a positive integer. But no reasonable estimate is supplied for the radius of the circle (about $z = 0$) on which (2) is convergent, the methods of proof being those referred to in the footnote to § 2.

The purpose of the first part of this appendix is to fill in somewhat this gap, by obtaining (*via* § 11) an estimate which is explicit enough and, at the same time, is free of one of the weak points criticized in that footnote, *viz*., of the step which involves the use of Cauchy's coefficient estimates (the "calcul des limites"). Still, the result to be obtained cannot possibly be of a final nature; in fact, two processess of majorization remain to be dispensed with.

In the latter part of this appendix, it will be shown that one at least of these two, substantially weakening, processes of majorization *can* be dispensed with (*via* § 1, rather than, as before, *via* § 11); so that just one of the three aspects criticized in the footnote to § 2 will ultimately remain. For it will turn out that, owing to the lemma of § 1, the majorization of the differential equation (1) by an "implicit equation" of the form $w = f(z,w)$, a majorization which since Briot and Bouquet is an essential point in all treatments of (1) (cf. the references in the footnote to § 2), can be avoided entirely.

The only remaining weak point will therefore be the majorization of (1) by a case of (1), with $\beta = 0$ but $a \geqq 0$ and $a_{mn} \geqq 0$ (the latter constants β, a, a_{mn} are not, of course, the same as in (1); the new a_{mn} is the absolute value of the old a_{mn}). But even this single process of majorization must prevent a result which is as sharp as possible (except as a result of majorization; cf. the first of my papers referred to in § 2). Correspondingly, what will be involved is only that (compartively straightforward) particular case of the lemma of § 1 in which the coefficients of the double power series $f(z,w)$ are $\geqq 0$.

If $h(z,w)$ is any power series, let $h^*(z,w)$ denote its *best majorant, i. e.*, put

$$(3)\qquad h^*(z,w)=\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}|b_{mn}|z^mw^n \text{ if } h(z,w)=\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}b_{mn}z^mw^n.$$

Thus $h^*(z,w)$ is convergent on a dicylinder

$$(4)\qquad |z|<a,\qquad |w|<b$$

if $h(z,w)$ is, but the function $h^*(z,w)$ need not be bounded on (4) if the function $h(z,w)$ is. Suppose however that, if $\phi(z,w)$ is the power series occurring in (1), the radii of the dicylinder (4) are chosen so small that not only $\phi(z,w)$ but also $\phi^*(z,w)$ will be bounded on (4). Next, in terms of the second of the constants occurring in (1), a constant β which can be complex but is, by assumption, not a positive integer, define a positive number $\gamma=\gamma(\beta)$ by placing

$$(5)\qquad \gamma=\min_{2\leqq n<\infty}|n-\beta|.$$

Finally, since 1 is a positive integer, hence $|\alpha/(1-\beta)|$, where α is the first of the constants occurring in (1), is a non-negative value distinct from ∞, it is possible to choose the radii of the dicylinder (4) so small that the inequality

$$(6)\qquad |\alpha/(1-\beta)|\,a^2+\phi^*(a,b)a/\gamma\leqq b$$

becomes satisfied (in fact, since α, β and $\gamma=\gamma(\beta)>0$ are fixed, and since $\phi(z,w)$, hence $\phi^*(z,w)$, vanishes at $(0,0)$ in the second (collective) order (of z,w), at least, the inequality (6) will be satisfied by a sufficiently small $a>0$ even if $b=a$). The explicit result, to be proved, can now be formulated as follows:

If β is not a positive integer, γ is defined by (5), *and $a>0$ is chosen so small that* (6) *holds for some $b=b_a>0$, then* (1) *possesses a (unique) regular solution $w(z)$, with $w(0)=0$, on a circle* $|z|<$ const. *the radius of which is not less than a.*

First, if (2) is substituted into (1), comparison of like powers of z supplies for $k>1$ the recursion formula

$$(7)\qquad (k-\beta)c_k=\Phi_k(c_1,\cdots,c_{k-1}),\qquad c_1=\alpha/(1-\beta),$$

where Φ_k is a polynomial (in $k-1$ variables), with coefficients which are polynomials in the coefficients a_{mn} of $\phi(z,w)$. Let $\Psi_k(c_1,\cdots,c_{k-1})$ denote the polynomial (with real, non-negative coefficients) which results if every a_{mn} is replaced by $|a_{mn}|$ in $\Phi_k(c_1,\cdots,c_{k-1})$. Then it is easily realized from the definitions, (3) and (5), of the symbol * and of the number γ that the sequence of the absolute values $|c_1|, |c_2|, \cdots$ of the numbers $c_1, c_2, \cdots$ defined by (7) is majorized by the (real, non-negative) sequence $C_1, C_2, \cdots$ defined by

$$(8) \qquad \gamma C_k = \Psi_k(C_1, \cdots, C_{k-1}), \qquad C_1 = |\alpha/(1-\beta)|,$$

where $k > 1$. On the other hand, it is clear from the definition of Ψ_k that substitution of (2) into

$$(9) \qquad \gamma w = \lambda z + \phi^*(z, w), \text{ where } \lambda = \gamma\,|\alpha/(1-\beta)|,$$

leads to the first or to the second of the relations (8) according as $k > 1$ or $k = 1$. Hence, in order to prove that (1) possesses a solution $w = w(z)$, satisfying $w(0) = 0$, which is regular on a given circle $|z| < a$, it is sufficient to prove that (9) possesses such a solution on that circle.

Next, if $f(z,w)$ is regular, and $|f(z,w)|$ is less than a constant M, on a dicylinder (4), and if $f(0,0) = 0$, then the equation $w = f(z,w)$ has on the circle $|z| < a$ a (unique) regular solution $w = w(z)$ satisfying $w(0) = 0$, provided that the inequality $M \leqq b/a$ is satisfied by a, b, M. For if all three constants a, b, M are normalized to be 1, then the assertion reduces to that of § 11. But if z, w and $w = f(z,w)$ are replaced by pz, qw and $rw = rf(z,w)$ respectively, where p, q, r are positive constants, then, by choosing the latter so as to render 1 the resulting values of a, b, M, the assertion follows.

Finally, let $w = f(z,w)$ be identified with what results if (9) is written in the form

$$(10) \qquad w = |\alpha/(1-\beta)|\, z + \phi^*(z,w)/\gamma.$$

Then it is clear that $|f(z,w)| < M$ holds on (4) if M denotes the value which the sum occurring on the right of (10) attains at $(z,w) = (a,b)$. But this choice of M reduces the inequality $M \leqq b/a$ to the inequality (6). Thus § 11, when applied to the majorant (10) of (1), supplies precisely that explicit form of the Briot-Bouquet theorem which was italicized after (6).

Unfortunately, what was used here from § 11 is substantially more on the surface than § 11 itself, since all coefficients of the double power series $f(z,w)$ are non-negative in the case (10) of $w = f(z,w)$. Without this circumstance, produced by the process of majorization, a result sharper than (6) would follow from § 11.

⁂

There is however an additional weak point in the majorization of (1) by (10). This point is the circumstance that the replacement of (7) by

(8), where γ is independent of k, implies the sacrifice of all the convergence-producing effects of the big factor $(k-\beta)\sim k\rightarrow\infty$ on the left of (7). But it turns out that this drastic step,[†] which goes back to Briot-Bouquet, can be avoided entirely.

Instead of the positive constant $\gamma=\gamma(\beta)$ defined by (5), introduce the positive constant $\mu=\mu(\beta)$ defined by

$$\mu=\max_{2\leqq n<\infty}|n-\beta|/n; \tag{11}$$

so that $\mu>0$, in contrast with $\gamma>0$, does not fail to involve the fact that $(k-\beta)$ is large for large k. Nevertheless, the situation is as follows:

The statement italicized after (6) *remains true if the factor* $1/\gamma$ *of the second term in* (6) *is replaced by the factor* $1/\mu$ *defined by*

$$\mu=\max_{2\leqq n<\infty}|1-\beta/n|$$

(*cf.* (5) *and* (11)).

In fact, it is clear from (11) and from the definition of Ψ_k that, instead of (8),

$$\mu k c_k=\Psi_k(c_1,\cdots,c_{k-1}),\qquad c_1=|a/(1-\beta)| \tag{8 bis}$$

can be used as a majorant system of (7). But it is also clear that this majorant system belongs to the solution (2) of the *differential* equation

$$\mu z w'=\lambda z+\phi^*(z,w),\ \text{where}\ \lambda=\gamma\,|a/(1-\beta)|, \tag{9 bis}$$

in the same way as (7) belongs to the solution (2) of the differential equation (1). Consequently, division by the constant $\mu>0$ shows that if the differential equation

$$zw'=f(z,w),\ \text{where}\ f(z,w)=|a/(1-\beta)|\,z+\phi^*(z,w)/\mu, \tag{10 bis}$$

possesses a solution $w=w(z)$, satisfying $w(0)=0$, which is regular on a given circle $|z|<a$, then such a solution $w(z)$ will exist, on the same circle, for (1) also. Consequently, the last italicized statement follows if § 1 is applied to (10 bis) in the same way as § 11 was applied to (10).

THE JOHNS HOPKINS UNIVERSITY.

[†] The possible effect of this step is well illustrated by the following example: If the recursion formula is $kc_k=c_{k-1}$, where $c_0=1$, then $w(z)=c_0+c_1z+\cdots$ is the solution $w(z)=\exp z$ of $w'=w$, whereas if the factor k is omitted on the left, then, since the recursion formula becomes $c_k=c_{k-1}$, there results the solution $w(z)=1/(1-z)$ of $w=zw$. But whereas $\exp z$ is an entire function, $1/(1-z)$ is not.

REMARKS TO TWO PREVIOUS PAPERS

(vol. 69, 1947, pp. 87-98 and vol. 71, 1949, pp. 587-594).*

By Aurel Wintner.

Let $f(t)$ be a continuous function on the (for instance, open) half-line $(0,\infty)$, and consider the three differential equations

$$(1) \quad x''-f(t)x=0, \qquad (2) \quad y'=y^2-f(t), \qquad (3) \quad (\log x)'=-y,$$

the second of which is equivalent to the first by virtue of the third if $x(t)\neq 0$ (Riccati). A classical result of A. Kneser states that if $f(t)\geqq 0$, then (1) has a solution $x(t)$ which is positive and non-decreasing on $(0,\infty)$ (so that

$$(4) \qquad x(t)>0 \text{ and } x'(t)\leqq 0, \text{ hence } x''(t)\geqq 0,$$

since $x''=fx$, $f\geqq 0$), and this solution $x(t)$ of (1) is unique up to a positive constant factor. If appropriate additional conditions are placed on $f(t)\geqq 0$, then more than (4) can be said about Kneser's solution $x(t)$. This is exemplified by the sequence of successive conditions which, in the first of my papers quoted in the title of this note, led to the following result: If $f(t)$ is totally monotone (in the sense of the Hausdorff-Bernstein theorem), then the same is true of $x(t)$. The following remarks consider similar but different implications which refer to Riccati's $y(t)$ in (3), rather than to $x(t)$ itself, as follows:

(i) If $f(t)\geqq 0$ on $(0,\infty)$, then (2) possesses one and only one solution $y(t)$ which exists and satisfies $y(t)\geqq 0$ on the whole of $(0,\infty)$.

(ii) If $f(t)\geqq 0$ is non-increasing and differentiable, i.e., $f'(t)\leqq 0$, then also $y'(t)\leqq 0$ holds.

(iii) In addition, $y''(t)\geqq 0$, if $f(t)\geqq 0$ and $f'(t)\leqq 0$ are subject to

$$(5) \qquad 16f^3(t)\leqq 27f'^2(t).$$

(iv) If $f(t)\geqq 0$ is convex (from below),† so that $f''(t)\geqq 0$, then, whether (5) is satisfied or not, the assertions, $y'(t)\leqq 0$ and $y''(t)\geqq 0$, of (ii) and (iii) imply the assumption, $f'(t)\leqq 0$, of (ii).

---

* Received July 22, 1957.

† The derivatives f', f'' (and y'') occurring in the wording of (iv) are meant in the sense customary in the theory of measurable convex functions: f' as a unilateral derivative, which is absolutely continuous, and f'' as the derivative of f' almost everywhere.

Note that the assertions of (i), (ii), (iii) on $y(t)$ and its derivatives claim for (2) what, *without* the additional assumptions placed on $f(t) \geqq 0$ in (ii) and (iii), the inequalities (4) ensure for (1) by virtue of $f(t) \geqq 0$ alone. In fact, (i), (ii), (iii) can be summarized by saying that

$$(6) \qquad f(t) \geqq 0, \qquad f'(t) \leqq 0$$

and (5) together imply that

$$(7) \qquad y(t) > 0, \qquad y'(t) \leqq 0, \qquad y''(t) \geqq 0$$

on $(0, \infty)$. On the other hand, neither the necessity nor the sufficiency of

$$(8) \qquad f(t) \geqq 0, \qquad f'(t) \leqq 0, \qquad f''(t) \geqq 0$$

for (7) follows from (iv).

It is easy to see that (8) cannot replace (6) and (5) for (7) (substantially more than this negation results from the example to be constructed at the end of this paper). On the other hand, it is not clear that (5) cannot be improved by diminishing the value of the absolute constant 27/4.

Proof of (i). It is seen from (3) that (i) is just a restatement of Kneser's theorem.

Proof of (ii). Draw in the half $t > 0$ of the (t, y)-plane the curves $C_1: y = y^*(t)$ and $C_2: y = -y^*(t)$, where $y^* = f^{\frac{1}{2}} \geqq 0$, and denote by P, Q, R the sets of those points of that half-plane which are situated, respectively, above C_1, between C_1 and C_2 (with the inclusion of the boundary $C_1 + C_2$), and below C_2. Then the solution curve $C: y = y(t)$, being, by (i), in the half-plane $y \leqq 0$, cannot have any point in P. If C had a point in R, then the method of the "curves of zero velocity" (cf. my note in the Quart. Journ. of Math. (Oxford), vol. 18 (1947), pp. 65-71) would lead to a situation which is contradicted by (2), since the "curves of zero velocity" are the present C_1 and C_2, and since, in view of the hypothesis of (ii), the (common) absolute value of the ordinates of C_1 and C_2 is a non-increasing function of t. Consequently, C stays in Q. In view of (2), this means that $y'(t) \leqq 0$, as claimed by (ii).

Proof of (iii). If (2) is differentiated and y' is substituted from (2) into the result, it follows that $y'' = 2\phi(y)$, where $\phi(y)$ denotes the case $a = f(t) \geqq 0$, $b = -\frac{1}{2}f'(t) \geqq 0$ of the cubic polynomial $y^3 - ay + b$. Since $y(t) > 0$, by (i), it follows that $y''(t) > 0$ if $\phi(y) = 0$ has no positive root (for then $\phi(y) > 0$ if $y > 0$, since $\phi(\infty) = \infty$). But $\phi(y) = 0$ has no positive root if $4a^3 < 27b^2$. Hence, for reasons of continuity, the assertion,

$y''(t) \geqq 0$, of (iii) follows even if the last $<$ is relaxed to $\leqq$. Since the resulting inequality between a and b is precisely the assumption of (iii), the assertion of (iii) follows.

Proof of (iv). Differentiation of (2) shows that $f' = 2yy' - y''$. Hence $f' \leqq 0$ is necessary for (7). But (7) is the assumption of (iv).

⁂

Let T denote the class of totally monotone functions $z(t)$ on $0 < t < \infty$, characterized by the existence of a Hausdorff-Bernstein integral representation or, equivalently, by the inequalities $(-D)^n z(t) \geqq 0$, where $n = 0, 1, \cdots$. The assertions of (i)-(iii) are that, under their assumptions on $f(t)$ and $f'(t)$, the first three of these inequalities are satisfied by the negative of the logarithmic derivative, $z = y(t)$, of the Kneser solution, $x = x(t)$, of (1). But one can ask whether *all* inequalities $(n = 0, 1, \cdots)$ follows for $z = y(t)$ if *all* of them are assumed for $z = f(t)$; i.e., whether $(f \in T) \Rightarrow (z \in T)$ is true for $z = y$. The question[*] is the more natural since, as mentioned after (4), the last $\Rightarrow$ is true for $z = x$. But it turns out to be false for $z = y$.

Actually, (I) $f \in T$ is necessary, but not sufficient, for $y \in T$, and the situation becomes just the opposite if (2) is replaced by (1), since (II) $f \in T$ is sufficient, but not necessary, for $x \in T$ (here $x(t)$ and $y(t)$ are Kneser's solution of (1) and the corresponding function (3) respectively).

First, if x is the function $1 + e^{-t}$, then $x \in T$. But $f = x''/x$, by (1), and so $f = e^{-t}/(1 - e^{-t})$ has on $(0, \infty)$ an expansion $c_1 e^{-t} + c_2^{-2t} + \cdots$, with $c_n = (-1)^{n-1}$, whereas $c_n \geqq 0$ ought to hold for every n (Hausdorff-Bernstein) if $f \in T$ were true. This proves the second part of (II). The first part of (II) is the result referred to after (4).

Next, if $y \in T$, then $y^2 \in T$ and $-y' \in T$, and so, if (2) is written in the form $f = y^2 - y'$, it follows that $f \in T$, as claimed by the first part of (I). Hence, only the second part of (I) remains to be proved.

To this end, let $y(t)$ be a power series $\Sigma a_n e^{-nt}$ which converges on $(0, \infty)$ (i.e., let $\limsup |a_n|^{1/n} \leqq 1$), choose $a_2 = -1$ but $a_n \geqq 0$ if $n \geqq 3$, and let a_0 and a_1 be positive numbers, the larger the better for the present. In any case, let $a_0 + a_1 \geqq 1$. Then $y(t) > 0$ on $(0, \infty)$, as required by (i). But since *not every* a_n is non-negative, it follows from the uniqueness of a Laplace-Stieltjes representation, and from the theorem Hausdorff-Bernstein, that $y \in T$ fails to hold. On the other hand, if $f(t)$ turns out to be a power series $\Sigma c_n e^{-nt}$ in which $c_n \geqq 0$ holds for *every* n, then $f \in T$ will be satisfied. This can however be arranged for, as follows:

---

[*] In the second of the notes quoted in the title of this paper, the question $y \in T$ was considered under the assumption that the coefficient function $f(t)$ of (1), instead of being non-negative as above, is non-positive on $(0, \infty)$. This situation is of a somewhat restricted scope, since, while (1) is non-oscillatory in every case $f(t) \geqq 0$, it will be oscillatory in a case $f(t) \leqq 0$ unless $-f(t) \geqq 0$ is "small." But unless (1) is non-oscillatory, it is clear from (3) that (2) will not possess any solution $y(t)$ which exists (as a finite-valued function) on the whole of $(0, \infty)$.

Substitution of $y(t) = \Sigma a_n e^{-nt}$ into the formulation $f = -y + y^2$ of (2) shows that $c_0 > 0$ and $c_1 > 0$ (if $a_0 > 0$ and $a_1 > 0$ are large enough), and that $c_n = na_n + \Sigma a_{n-k} a_k$ if $n \geqq 1$, where $0 \leqq k \leqq n$. Since $a_2 = -1$, it is also clear that $c_2 \geqq 0$ (if $a_0 > 0$ and $a_1 > 0$ are large enough), and that $c_n \geqq 0$ will hold for $n \geqq 3$ if and only if

$$na_n + \sum_{k=0}^{n}{}^{*} a_{n-k} a_k \geqq 2a_{n-2}, \qquad (n = 3, 4, \cdots), \tag{9}$$

where the * refers to the omission of both summation indices $k = 2$, $k = n - 2$. The contribution of the latter would be $a_2 a_{n-2} + a_{n-2} a_2 = -2a_{n-2}$ but is written on the right of the inequality (9).

Note that no a_m occurring on the left of (9) has the index $m = 2$ and so, since a_2 is the only negative a_m, all terms of the sum Σ^* are non-negative. Hence, if the a-values having an index less than a fixed n have been determined, then, since a_n occurs only on the left of (9), the n-th of the inequalities (9), where $n \geqq 3$, can be satisfied by choosing a_n large enough. The only precaution needed is that the successive choice of the a_n-values should not make them too large, but such as to be compatible with the condition $\limsup a_n^{1/n} \leqq 1$, the condition needed for the convergence of $y(t) = \Sigma a_n e^{-nt}$ on $(0, \infty)$. But it is readily seen from the presence of the large factor $(= n)$ in the first term of (9) that this condition can be satisfied by the successive choice of $a_3 > 0, a_4 > 0, \cdots$, the initial values a_0, a_1 being positive and arbitrarily large, while $a_2 = -1$.

(I) and (II) imply that $f \in T$ is sufficient for $x \in T$ but not for $y \in T$. This contains of course the fact that (without any reference to an f) the definition (3) fails to be such as to lead from $x \in T$ to $y \in T$; but this fact is made trivial by the example $x = 1 + e^{-t}$, since $y \in T$ is prevented by $y = e^{-t}/(1 + e^{-t}) = e^{-t} + be^{-2t} + \cdots$, where $b = -1 < 0$. All that is true is that $y \in T$ is sufficient for $x \in T$ if $x > 0$ (without any reference to an f). For if $x(t)$ is a positive function satisfying a differential equation of the form $x' = -y(t)x$ with some $y \in T$, then, as is well-known, successive differentiations lead, by an induction, from $(-D)^n y \geqq 0$ to $(-D)^n x \geqq 0$.

THE JOHNS HOPKINS UNIVERSITY.

ON THE NON-VANISHING OF EULER PRODUCTS.*

By Norbert Wiener and Aurel Wintner.

Let a function $\chi = \chi_p$, defined on the set of all prime numbers p, be such as to satisfy the following two conditions:

$$(1) \qquad -1 \leqq \chi_p \leqq 1$$

(e.g., $\chi_p^2 = |\chi_p|$, i.e., $\chi_p = -1, 0, 1$) and

$$(2) \qquad f(s) \text{ is meromorphic on } \sigma = 1,$$

if $f(s)$ the Euler product

$$(3) \qquad f(s) = \Pi(1 - \chi_p/p^s)^{-1} \qquad (\sigma > 1).$$

By the condition (2) is meant the assumption that there exist an open domain D in the s-plane and a meromorphic function $f(s)$ on D in such a way that D contains the half-plane $\sigma \geqq 1$ (but possibly no half-plane $\sigma \geqq 1 - \epsilon$, where $\epsilon > 0$) and that $f(s)$ is identical on the half-plane $\sigma > 1$ with the function which is there represented by the product (3); a function which, in view of (1), is regular (and non-vanishing) for $\sigma > 1$. On the other hand, the condition (1) means that if χ is extended from primes to positive integers by the assignments $\chi_1 = 1$ and $\chi_n \chi_m = \chi_{nm}$ (so that (3) becomes identical with the absolutely convergent Dirichlet series $\Sigma \chi_n/n^s$ if $\sigma > 1$), then the resulting real-valued representation χ_n of the multiplication on the semi-group of the positive integers n is a bounded representation (in fact, $\limsup |\chi_n| = \infty$ unless $|\chi_n| \leqq 1$ for every n). The two extreme cases allowed by (1) and (2) result if $\chi_p = 1$ and $\chi_p = -1$ (for every p); in fact, since (3) then reduces to

$$(4) \qquad \Pi(1 - p^{-s})^{-1} = \zeta(s) \text{ and } \Pi(1 + p^{-s})^{-1} = \zeta(2s)/\zeta(s),$$

(2) is satisfied in both cases.

The following considerations were suggested by a point occurring in Hadamard's, and also in de la Vallée Poussin's, proof of

$$(5) \qquad \zeta(s) \neq 0 \text{ on } \sigma = 1.$$

---

* Received June 29, 1957.

The point in question is the following: Besides the case $f(s) = \zeta(s)$ of (2), it is assumed in the proof of (5) that $\zeta(s)$ *is regular* (*rather than just meromorphic*) *at every* $s = 1 + it \neq 0$. It is this fact from which the negation of (5) leads to a contradiction, since what is actually proved is the following: If $\zeta(s)$ would have a zero $s = 1 + it_0$, then it would also have some pole $s = 1 + it^0$ distinct from the pole $s = 1$ (in fact, it is shown that t^0 could be chosen to be $2t_0$; cf., e.g., [1], pp. 29-30). Accordingly, the proof of (5) fails to succeed if all that is known for the case $f(s) = \zeta(s)$ of (3) is the following pair of assumptions: (2) and

(6) $f(s)$ has a pole at $s = 1$.

There is quite another proof of (4), the function-theoretical proof adapted by Ingham from Landau's proof [2] of Dirichlet's theorem $L(1) \neq 0$ (in Landau's function-theoretical proof, $L(s)$ belongs to a real character); cf. [1], p. 89. But this proof is even more restrictive than the preceding one, since what is now assumed is the regularity of $f(s)$ at every point $s \neq 1$ of the half-plane $\sigma \geqq \frac{1}{2}$ (on the boundary line $\sigma = \frac{1}{2}$, less than regularity is needed).

Thus it is natural to ask whether

(7) $f(s) \neq 0$ on $\sigma = 1$,

the generalization of (5) for an arbitrary case (1) of (3), must or need not be true if only (2) and (6) are assumed. For, as seen above, the classical argument applies only if (1) is retained but (2) is strengthened to the hypothesis that

(8) $f(s)$ is regular on $\sigma = 1$ if $s \neq 1$.

The purpose of this note is to show that the answer to the question, just raised, is in the affirmative; in other words, that (7) remains true if (8) is relaxed to (2). Curiously enough, (8) proves to be a consequence of the other hypotheses; so that the situation is as follows:

(I) *In terms of a sequence* $\chi_2, \chi_3, \cdots$ *satisfying* (1), *define on the open half-plane* $\sigma > 1$ *a* (*regular, non-vanishing*) *function* $f(s)$ *by the corresponding Euler product* (3), *and suppose that, as* $\sigma \rightarrow 1 + 0$, *the function* $f(s)$ *behaves in such a way that conditions* (2) *and* (6) *are satisfied. Then both* (8) *and* (7) *hold.*

Actually, (I) is not the final result, since the assumption (6) of (I) proves to be superfluous. This is the content of the theorem at the end of this paper.

Although (I) contains (5), there will result no new proof of (5), since (5), along with

$$1/\zeta(s) \neq 0 \text{ on } \sigma = 1 \text{ if } s \neq 1 \tag{9}$$

(that is to say, the regularity and the non-vanishing of $\zeta(1+it)$ for $0 < t < \infty$), will be granted in the proof of (I). What will directly be proved is not (I) itself but the following variant of (I):

(II) *The assertions of* (I) *remain true if its assumption* (6) *is replaced by the assumption*

$$f(1) = 0 \tag{10}$$

(and all the other assumptions of (I) are retained).

Proof of (II). For $-\infty < t < \infty$, let j_t denote the index (the logarithmic residue) of $f(s)$ at $s = 1 + it$, and let J_t belong to

$$F(s) = \zeta(s) f(s) \tag{11}$$

in the same way as j_t belongs to $f(s)$. Since (2) is assumed for $f(s)$ itself and for $f(s) = \zeta(s)$, it is clear from (5), (9) and (11) that $j_t = J_t$ for $t \neq 0$. Since the assertions, (8) and (7), of (II) are equivalent to $j_t = 0$ for $t \neq 0$, and since (10) and (11) imply that $J_0 = 0$ (for $\zeta(s)$ has a simple pole at $s = 1$), it follows that (II) will be proved if it is shown that

$$|J_t| \leqq J_0 \qquad (J_0 = 0) \tag{12}$$

holds for every t. But the truth of (12) can be concluded by an elementary argument (cf. [3], where (8), rather than just (2), is assumed, (10) is retained, and (1) is generalized to complex-valued χ_p, with $|\chi_p| \leqq 1$).

In order to prove (12), note that, if $\sigma > 1$, logarithmic differentiation of (3) leads to

$$-f'/f(s) = \sum_p \sum_{k=1}^{\infty} (\chi_p \log p)/p^{ks}. \tag{13}$$

If (13) is added to the case $\chi_p = 1$ of (13), it follows from (11) and from the first of the relations (4) that, if $\sigma > 1$,

$$-F'/F(s) = \sum_p \sum_{k=1}^{\infty} a_p/p^{ks}, \tag{14}$$

where

$$(15)\qquad a_p = (1+\chi_p)\log p.$$

But since (15) and (1) imply that $a_p \geqq 0$, it is clear from (11) that, if $\sigma > 1$,

$$(16)\qquad |(\sigma-1)F'/F(\sigma+it)| \leqq |(\sigma-1)F'/F(\sigma)| \text{ for } -\infty < t < \infty.$$

If $\sigma \rightarrow 1+0$, then (16) goes over into $|J_t| = |J_0|$, and so (12) follows from the parenthetical equality in (12).

This completes the proof of (II).

Actually, the following extension of (II) was also proved:

(II*) *The assertions of* (II) *remain true if its assumption* (1) *is replaced by the unilateral restriction* $-1 \leqq \chi_p$, *provided that the Euler product* (3) *is uniformly convergent on every compact subset of the half-plane* $\sigma > 1$.

The latter proviso (which, since χ_p is bounded from below, is satisfied if, though not only if, $\chi_p \leqq$ Const. for some Const.) cannot of course be omitted. But then the restriction $-1 \leqq \chi_p$ will suffice in the preceding proof, since, in view of (15), this unilateral restriction is equivalent to $a_p \geqq 0$.

Much deeper lies the following fact:

(II bis) *Under the assumptions of* (II), *and even those of* (II*), *the function* $f(s)$ *possesses an analytic continuation which is meromorphic on some half-plane* $\sigma > 1-\epsilon$, *where* $\epsilon = \epsilon_f > 0$, *and* $f(s)$ *does not vanish at any point* $s \neq 1$ *of this half-plane* $\sigma > 1-\epsilon$.

[REMARK. *If it is true that* $\zeta(s)$ *has no zero on some open half-plane containing the line* $\sigma = 1$ (*for instance, if Riemann's hypothesis is true*) *then, in* (II bis), *the word "meromorphic" can be replaced by "regular."*]

In fact, since $\zeta(s)$ has a simple pole at $s=1$, it is clear from (2), (10) and (11) that, if $\epsilon > 0$ is small enough, $F(s)$ is regular at every point of the half-line $s > 1-\epsilon$, and that $F(s)$ can have a zero on such a half-line only if $s=1$ is a multiple zero of $f(s)$ (in fact, (3) does not vanish for $s > 1$). But $f(s)$ cannot have a multiple zero at $s=1$, since, if $s > 1$ and $-1 \leqq \chi_p$, it is clear from (3) that

$$f(s) \geqq \Pi(1+p^{-s})^{-1} \sim \text{const.}\,(s-1) \text{ as } s \rightarrow 1-0,$$

where const. $= \zeta(2) > 0$, by the second of the relations (4).

Accordingly, $F(s)$ is a regular and non-vanishing function, and so the logarithmic derivative of $F(s)$ is a regular function, on some half-line $s > 1 - \epsilon$. Since $a_p \geqq 0$, it now follows from Landau's theorem (on Dirichlet series $\sum c_n/n^s$ with $c_n \geqq 0$), a theorem referred to but not used above, that the Dirichlet series (14) must converge for $s > 1 - \epsilon$ and, therefore, for $\sigma > 1 - \epsilon$. Consequently, the logarithmic derivative of $F(s)$ is a regular function, and therefore $F(s)$ is a non-vanishing regular function, on the half-plane $\sigma > 1 - \epsilon$. In view of (11), this proves both (II bis) and the Remark following (II bis).

Proof of (I). If χ_p is replaced by $-\chi_p$ (for every p), then the assumption (1) remains unaltered but (3) becomes replaced by

$$f^*(s) = \Pi(1 + \chi_p/p^s)^{-1}. \tag{17}$$

The connection between (3) and (17) is involutory. But while it is clear from (1) that (17) represents a non-vanishing regular function for $\sigma > 1$, it is not quite obvious that (2), too, is an involutory property; in other words, that

$$f^*(s) \text{ is meromorphic on } \sigma = 1 \tag{18}$$

if (2) is assumed. It turns out, however, that (18) follows from (2) and is, therefore, equivalent to (2).

First, since (2) remains true if $f(s)$ is replaced by $1/f(s)$, more than (18) will follow if it is ascertained that the quotient of $f^*(s)$ and $1/f(s)$ is a non-vanishing regular function on the line $\sigma = 1$. But (3) and (17) show that, if $\sigma > 1$, this quotient is identical with

$$f(s)f^*(s) = \Pi(1 - \chi_p^2/p^{2s})^{-1}. \tag{19}$$

On the other hand, it is clear from (1) that (19) is a regular and non-vanishing function on the half-plane $\sigma > \frac{1}{2}$ and, therefore, on the line $\sigma = 1$. [This conclusion is curious, since, by placing either $\chi_p = 1$ or $\chi_p = 0$, and making the alternative choice in an appropriate ("lacunary") manner, it is easy to obtain a pair of functions (1), (17), the factors on the left of (19), which are regular on the half-plane $\sigma > \theta$ but become singular at every point of the line $\sigma = \theta$, where $\frac{1}{2} < \theta < 1$, rather than $\theta = \frac{1}{2}$.]

Let $(1^*), (2^*), \cdots$ denote what results if $f(s)$ is replaced by $f^*(s)$, and χ_p by $-\chi_p$, in $(1), (2), \cdots$ respectively. Then, as just shown, (1) and (2) together are equivalent to (1^*) and (2^*) together. Since (II) has already been proved, it follows that (1^*), (2^*) and (10^*) imply both (8^*) and (7^*).

But the quotient of $f^*(s)$ and $1/f(s)$ and, hence, the quotient of $1/f(s)$ and $f^*(s)$, was seen to be a non-vanishing regular function on the line $\sigma = 1$. Hence (8*) and (7*) are equivalent to (7) and (8) respectively and so, since (10) goes over into (6) if $f(s)$ is replaced by $1/f(s)$, the proof of (I) is now complete.

* * *

If $f(s)$ is an L-function of Dirichlet belonging to a real non-principal character (so that, in particular, (1) and (3) hold for a certain χ_p which is capable of the three values $-1, 0, 1$ only), and if the meromorphic (rather than the regular) behavior of $L(s)$ on $\sigma = 1$ is assumed, then, since $L(1) \neq 0$ (Dirichlet) but $L(1) \neq \infty$, neither the non-vanishing nor the regularity of $L(s)$ on $\sigma = 1$ can be concluded from (I) and (II) together. Hence there arises the question whether or not (7) and (8) remain true if (1) and (2) are retained for (3) but (6) and (10) are replaced by

$$(20) \qquad 0 \neq f(1) \neq \infty$$

(or, what in view of (1) and (3), where $\sigma > 1$, is the same thing, by $0 < f(1) < \infty$). It will be shown that the answer to this question is affirmative:

(III) *The assertions of* (I) *remain true if* (6) *is replaced by* (20).

In order to prove (III), it will be sufficient to show that, under the assumptions of (III), the line $\sigma = 1$ cannot contain a zero of $f(s)$. For if this is granted, then the remaining assertion of (III), according to which $f(s)$ cannot have a pole on $\sigma = 1$, will follow in the same way in which (I) and (II) were proved to be equivalent (that is, by applying (17) and (19) in the same way as above). Hence it is sufficient to assume that $f(s)$ has a zero $s = 1 + ia$ on $\sigma = 1$ and to show that the existence of at least one such real number a leads to a contradiction.

First, $a \neq 0$, since $f(1) \neq 0$. Next, since $f(s + ia) = 0$ at $s = 1$, and since (1) and (3) imply that $f(1 + it)$ and $f(1 - it)$ are complex conjugate values, it is clear that the function

$$(21) \qquad G(s) = \zeta^2(s) f(s + ia) f(s - ia)$$

(which, in view of (2), is meromorphic on $\sigma = 1$) will have at $s = 1$ neither a zero nor a pole if the zero $s = 1 + ia$ of $f(s)$ is a simple zero (the factor $\zeta^2(s)$ of (21) has a double pole at $s = 1$). But the argument applied in the proof of (II bis) also shows that $f(s)$ cannot have a multiple zero on $\sigma = 1$ (simply because (1) and (3) imply that, if $\sigma > 1$,

$$|f(\sigma + it)| \geqq \Pi(1 + p^{-})^{-1} = \zeta(2\sigma)/\zeta(\sigma) > \text{Const.}(\sigma - 1)$$

holds for every t and for a certain Const. > 0). Accordingly, if K_t denotes the logarithmic residue of $G(s)$ at the point $s = 1 + it$, then $K_0 = 0$.

It will be shown that

$$(22) \qquad |K_t| \leqq |K_0|$$

holds for every t. In view of $K_0 = 0$, this will prove that $K_t = 0$ holds for every t. It will therefore follow from (5), (9) and (21) that $f(s + ia)f(s - ia)$ is of index 0, and so a non-vanishing regular function, at every point $s \neq 1$ of the line $\sigma = 1$. Since $f(1 + it)$ and $f(1 - it)$ are complex conjugates, and since $a \neq 0$, it now follows that $f(s)$ is regular (rather than just meromorphic) on $\sigma = 1$. But since $s = 1 + ia$ and $s = 1 - ia$ are two distinct zeros of $f(s)$, this contains a contradiction. In fact, it was shown in [3] that if (1) (or, in the complex case, just $|\chi_p| \leqq 1$) holds in (3), where $\sigma > 1$, and if the function $f(s)$ remains regular at every point of $\sigma = 1$, then $f(s)$ cannot have more than one zero on $\sigma = 1$.

In view of this contradiction, the proof of (III) will be complete if the truth of (22) is proved (for every t). But (22) can be proved, along the lines of the proof of (12), as follows:

If $s = \sigma + it$, where $\sigma > 1$, is replaced in (13) once by $s + ia$ and once by $s - ia$, it follows, by addition, that the logarithmic derivative of $f(s + ia)f(s - ia)$ is

$$(23) \qquad -\sum_p \sum_{k=1}^{\infty} (\lambda_{p,k} \log p)/p^{ks}, \text{ where } \lambda_{p,k} = 2\chi_p \cos(ak \log p).$$

On the other hand, it follows from the first of the relations (4) that the logarithmic derivative of $\zeta^2(s)$ results from (23) if χ_p and a are replaced by 1 and 0 respectively. If the resulting series is added to (23) itself, then the definition, (21), of $G(s)$ shows that

$$(24) \qquad -G'/G(s) = \sum_p \sum_{k=1}^{\infty} b_{p,k}/p^{ks} \text{ for } \sigma > 1,$$

where

$$(25) \qquad b_{p,k} = 2\mu_{p,k} \log p, \qquad \mu_{p,k} = 1 + \chi_p \cos(ak \log p).$$

But it is seen from (25) and (1) that $b_{p,k} \geqq 0$. Hence it is clear from (24) that (16) remains true if F is replaced by G. Consequently, (22) follows by letting $\sigma - 1 \to +0$.

Since this completes the proof of (III), the final result is as follows:

THEOREM. *If there is assigned to every prime p a value* χ_p *satisfying* $-1 \leqq \chi_p \leqq 1$, *and if the function* $f(s)$, *defined for* $\sigma > 1$ *by the Euler product* $f(s) = \Pi(1 - \chi_p/p^s)^{-1}$, *remains meromorphic at every point of the line* $\sigma = 1$, *then* $f(s)$ *is a regular and non-vanishing function at every point* $s \neq 1$ *of the line* $\sigma = 1$.

This theorem, which is equivalent to (I), (II) and (III) together, can be completed by the further information supplied by (II bis) and (II*) [and also by the hypothetical information contained in the Remark formulated after (II bis)].

MASSACHUSETTS INSTITUTE OF TECHNOLOGY,
THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] A. E. Ingham, *The distribution of primes*, Cambridge Tracts, no. 30, 1932.

[2] E. Landau, "Ueber einen Satz von Tschebyscheff," *Mathematische Annalen*, vol. 61 (1905), pp. 527-550.

[3] A. Wintner, "On the non-vanishing of certain Dirichlet series," *American Journal of Mathematics*, vol. 74 (1952), pp. 723-725.

LOCAL CONTRACTIONS AND A THEOREM OF POINCARÉ.*[1]

By SHLOMO STERNBERG.

One of the earliest treatments of the problem of normal forms for a system of n differential equations at a singular point occurs, at least implicitly, in Poincaré's thesis [6], pp. XCIX-CV (cf. also Picard [5]). In his thesis, Poincaré is concerned with those analytic partial differential equations of first order for which the Cauchy-Kowalewsky theorem does not apply. An important lemma in his considerations is the following: Given n analytic functions X_i of n complex variables x_j which are defined in some neighborhood of the origin and such that $X_i = \lambda_i x_i +$ higher order terms, consider the partial differential equations

$$X_1 \partial y_j/\partial x_1 + X_2 \partial y_j/\partial x_2 + \cdots + X_n \partial y_j/\partial x_n = \lambda_j y_j. \tag{1_j}$$

Then if

(i) all the λ_i lie in the same open half-plane about the origin

and

(ii_j) $\lambda_j \neq \sum m_i \lambda_i$ for any non-negative integral m_i such that $\sum m_i > 1$,

equation (1_j) has an analytic solution in some neighborhood of the origin. Now (1_j) is the j-th partial differential equation that a change of coordinates

$$y_i = y_i(x_1, x_2, \cdots, x_n) \qquad (i = 1, 2, \cdots, n) \tag{2}$$

must satisfy in order that it transform the system of ordinary differential equations

$$dx_i/dt = X_i(x_1, x_2, \cdots, x_n) \tag{3}$$

into the linearized form

$$dy_i/dt = \lambda_i y_i. \tag{4}$$

---

* Received March 11, 1957.

[1] This paper was written while the author was a Temporary Member of the Institute of Mathematical Sciences, New York University, during the academic year 1956-57. This Temporary Membership Program is supported by the National Science Foundation. Reproduction in whole or in part permitted for any purpose of the United States Government.

7

Thus if we denote by (ii) the totality of conditions (ii_j) for all j we can rephrase Poincaré's theorem as follows: Given a system of analytic differential equations (3) defined near the origin such that $X_i(0, 0, \cdots, 0) = 0$ and whose matrix of linear terms is diagonizable with eigenvalues λ_i satisfying (i) and (ii), then there exists an analytic change of coordinates (2) transforming (3) into (4).

Poincaré's proof of this theorem is a straightforward application of the Cauchy majorant method; condition (ii) implies the existence of a formal power series solution and (i) implies convergence. In this paper we shall deal with the problem of normal forms for real non-analytic differential equations for which there is, of course, no majorant method. Our approach will be of a geometrical nature and will deal with the flow generated by (3) rather than with (3) itself. If we examine condition (i) for the case of real differential equations, we observe that since every complex eigenvalue occurs along with its complex conjugate, the only admissible half planes are the right and left half planes. Substituting $-t$ for t, if necessary, we can replace (i) by

$$(\text{i}_R) \qquad \operatorname{Re}\lambda_j < 0 \quad \text{for all } j.$$

But (i_R) implies that the flow generated by (3) is a one-parameter semigroup of contractions in some neighborhood of the origin, i. e., that all points sufficiently close to the origin tend to the origin with increasing time. In what follows we shall obtain normal forms for smooth contractions in Euclidean n-space, that is, we shall obtain invariants for C^n contractions under inner automorphisms of the group of local C^k changes of coordinates. In addition to supplying information on the problem of normal forms for differential equations, our results generalize (to n dimensions and the non-analytic case) certain results of Lattès [3] on analytic surface transformations. We shall also obtain a generalization of the results of [8] on invariant curves to n dimensions.[2]

2. Before dealing with the problem of normal forms for contractions, we shall show that the problem is of an entirely different nature if no smoothness assumptions are made. This remark which is not essential in the sequel, follows from the fact that any two orientation preserving contractions in n-space are equivalent if the group of orientation preserving homeomorphisms of the $(n-1)$-sphere is arc-wise connected. This property is trivial for spheres of zero and one dimensions and is assured by a known theorem of H. Kneser in two dimensions. If there exists an n not satisfying the above condition, then the statement of Theorem 1 would have to be modified to take this fact into account. At any event, the structure of the mapping of the n-sphere has no effect on the following paragraphs.

---

[2] These results are an outgrowth of ideas contained in my thesis which was written under the direction of Professor Wintner.

THEOREM 1. *Let S and T be two orientation preserving homeomorphisms of some neighborhood of the origin in Euclidean n-space into itself such that*

$$\| Sx \| < \| x \| \text{ and } \| Tx \| < \| x \|, \tag{5}$$

where $\| \cdot \|$ is the ordinary Euclidean norm and where n satisfies the conditions preceding the theorem. Then there exists a homeomorphism R of some neighborhood of the origin onto itself keeping the origin fixed and such that

$$RSR^{-1} = T. \tag{6}$$

Proof. Let $\mathcal{S}$ denote some sphere which, together with its interior, $\mathfrak{B}$, is contained in the domain of definition of S and T. In virtue of (5)

$$T^{n+1}(\mathfrak{B}) \subset T^{n}(\mathfrak{B}) \text{ and } S^{n+1}(\mathfrak{B}) \subset S^{n}(\mathfrak{B})$$

so that we can write

$$\mathfrak{B} = \cup (T^{n}(\mathfrak{B}) - T^{n+1}(\mathfrak{B})) \text{ and } \mathfrak{B} = \cup (S^{n}(\mathfrak{B}) - S^{n+1}(\mathfrak{B})). \tag{7}$$

We define R to be the identity map on $\mathcal{S}$ and to map $\mathfrak{B} - S(\mathfrak{B})$ homeomorphically onto $\mathfrak{B} - T(\mathfrak{B})$ in such a manner that $R(Sx) = Tx$ for all x on $\mathcal{S}$. This can clearly be done since S and T are both homeomorphisms and by the assumptions concerning n. We now define R inductively to map $S^{n}(\mathfrak{B}) - S^{n+1}(\mathfrak{B})$ onto $T^{n}(\mathfrak{B}) - T^{n+1}(\mathfrak{B})$ by the equation

$$RS = TR. \tag{8}$$

If we set $R(0) = 0$ then, by (7) R is defined on all of $\mathfrak{B}$. Furthermore, since R was defined so as to be continuous at $S(\mathcal{S})$, it is a homeomorphism of $\mathfrak{B}$ onto itself satisfying (8), and hence (6) proving the theorem.

3. As soon as we restrict our group of local changes of variable to be of class C^1, Theorem 1 becomes false. In fact, there is a natural homomorphism of the group of local C^1 homeomorphisms onto the group of all non-singular n by n matrices: $T \rightarrow J(T)$ where $J(T)$ is the Jacobian matrix of the transformation T at the origin. The next conjecture would be that a normal form for $J(T)$ would be a suitable normal form for T. Now for the one dimensional case it was shown in [9] that if the linear operator $J(T)$ is a contraction and T is of class C^{k+1} $(k \geqq 1)$ then T can be linearized by a change of coordinates of class C^k. However this is not true in the n-dimensional case. In fact we shall exhibit an analytic contraction of the plane which can not be linearized by any transformation of class C^2 having a non-vanishing Jacobian at the origin. Consider the transformation

$$x_1 = a^2x + y^2, \qquad y_1 = ay. \tag{9}$$

We wish to show that there is no C^2 transformation

$$\xi = f(x, y), \qquad \eta = g(x, y) \tag{10}$$

such that in the ξ, η coordinates (9) assume the form

$$\xi_1 = a^2\xi, \qquad \eta_1 = a\eta. \tag{11}$$

In order for (10) to transform (9) into (11) f must satisfy the functional equation

$$f(a^2x + y^2, ay) = a^2f(x, y). \tag{12}$$

taking the partial derivative of both sides of (12) with respect to y gives

$$2yf_x(a^2x + y^2, ay) + af_y(a^2x + y^2, ay) = a^2f_y(x, y). \tag{13}$$

Setting $x = y = 0$ in (13) yields

$$f_y(0, 0) = 0. \tag{14}$$

Differentiating (13) with respect to y and setting $x = y = 0$ gives

$$f_x(0, 0) = 0. \tag{15}$$

But (14) and (15) imply that the Jacobian of (10) vanishes at the origin. Thus (9) can not be linearized.

4. In the n-dimensional case, the problem of finding normal forms for smooth transformation splits into two parts: one of a purely formal nature and the other analytic in character. In this section we shall deal with the formal part; our main goal being to bring every transformation satisfying certain formal conditions analogous to (i) into a prepared form so that the analytic considerations of the following section apply. Before proceeding with the calculations we shall make some remarks about the formalism in general. Let T^k denote the set of all C^k homeomorphisms defined in some neighborhood of the origin in n space keeping the origin fixed and having a non-vanishing Jacobian there. Given any two transformations A and B in T^k, we can compose them to form a third transformation $C = B \cdot A$ in T^k provided that we restrict attention to a sufficiently small neighborhood N of the origin. In order to be able to define C on N, N must be contained in the domain of A and such that $A(N)$ is contained in the domain of B. In order to avoid such difficulties, we can introduce the equivalence relation '$A \equiv B$ if A is identical with B on some sufficiently small neighborhood of the origin.' The elements of the coset space of T^k with respect to this equivalence relation form a group G^k known as the group of local C^k transformations. Now let P^k $(1 \leqq k \leqq \infty)$ denote the set of n-tuplets of real polynomials (formal power series) without constant terms in n real variables, which have terms of degree at most k. Then $P^1 \subset P^2 \subset \cdots \subset P^k \subset \cdots \subset P^\infty$. Let $\mathcal{J}^k$ denote the operator which truncates the n-tuplets of formal power series at their terms of degree k;

$$\mathcal{J}^k(\cdot\cdot\cdot, \sum_{i_j=1}^{\infty} a^i{}_{i_1\cdots i_n} x_1{}^{i_1} \cdot\cdot\cdot x_n{}^{i_n}, \cdot\cdot\cdot)$$
$$= \mathcal{J}^k(\cdot\cdot\cdot, \sum^{i_1+\cdots i_n \leqq k} a^i{}_{i_1\cdots i_n} x_1{}^{i_1} \cdot\cdot\cdot x_n{}^{i_n}, \cdot\cdot\cdot).$$

Then P^k has a natural multiplication defined on it, namely substitution followed by truncation of order k. If F^k denotes those elements of P^k whose matrix of linear terms is non-singular, then F^k is a group under this multiplication. The truncation operator $\mathcal{J}^k$ provides a canonical homomorphism of F^s onto F^k for $s > k$. Furthermore there is a natural homomorphism of G^k onto F^k once coordinates are chosen in Euclidean space, given by sending every mapping

$$(x_1, \cdot\cdot\cdot, x_n) \rightarrow (f_1(x_1, \cdot\cdot\cdot, x_n), \cdot\cdot\cdot, f_n(x_1, \cdot\cdot\cdot, x_n))$$

into the n-tuple whose elements are the Taylor expansions of the f_i at the origin of order k. We will now state a sufficient condition for an element of F^k to be linearizable by inner automorphisms of F^k. Since the mapping T^k is a homomorphism onto, it is sufficient for us to prove the result for F^∞.

LEMMA 1. *Let T be an element of F^k whose matrix of linear terms has no multiple elementary divisors and whose (possibly complex) eigenvalues $s_1, s_2, \cdot\cdot\cdot, s_n$ satisfy*

(II) $s_i \neq s_1{}^{m_1} s_2{}^{m_2} \cdot\cdot\cdot s_n{}^{m_n}$ *for any non-negative integral m_j such that*

$$\sum m_j > 1.$$

Then T is equivalent to its matrix of linear terms by an inner automorphism of F^k.

Since our groups are real, if complex eigenvalues do occur, they occur in pairs of complex conjugates. In that case, it is convenient to modify the group F^k by replacing the pair of real coordinates corresponding to the complex eigenvalues by a pair of conjugate complex variables and to allow complex formal power series satisfying certain symmetry (reality) conditions. This procedure is explained in detail in Birkhoff [1], pp. 60-63. In what follows, these symmetry conditions are automatically verified for the series that arise in virtue of the method of their construction. The convenience of introducing the complex coordinates is, of course, that it allows us to diagonalize the matrix of linear terms. We thus assume that T has the form

$$(s_1x_1 + \sum t^1_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}, \cdots, s_nx_n + \sum t^n_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}),$$

where all the series start with terms of degree at least two. We wish to find an $R = (r_1, \cdots, r_n)$ where the r_i are formal power series such that $RTR^{-1} = S = (s_1x_1, \cdots, s_nx_n)$. We can assume that the matrix of linear terms of R is the identity matrix and rewrite the desired equation as $RT = SR$ or

$$\begin{aligned} & s_i(x_i + \sum r^i_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}) \\ (16) \qquad & = s_ix_i + \sum r^i_{i_1\cdots i_n}(s_1x_1)^{i_1}\cdots(s_nx_n)^{i_n} + \sum t^i_{j_1\cdots j_n}x_1^{i_1}\cdots x_n^{i_n} \\ & + R_i(\sum t^1_{j_1\cdots j_n}x_1^{i_1}\cdots x_n^{i_n}, \cdots, \sum t^n_{j_1\cdots j_n}x_1^{i_1}\cdots x_n^{i_n}), \end{aligned}$$

where the $r_i = x_i + \sum r^i_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n} = x_i + R_i$. If we compare the coefficients of $x_1^{i_1}\cdots x_n^{i_n}$ in (16), we obtain

$$(17) \qquad s_ir^i_{i_1\cdots i_n} = (s_1^{i_1}\cdots s_n^{i_n})r^i_{i_1\cdots i_n} + P^i_{i_1\cdots i_n},$$

where $P^i_{i_1\cdots i_n}$ is a polynomial in those $r^j_{j_1\cdots j_n}$ such that $\sum j_k < \sum i_k$. By (II), we can solve (17) for $r^i_{i_1\cdots i_n}$. This allows us to determine consecutively all the coefficients of the r_i so as to satisfy (16), proving the lemma.

5. In this section we shall deal with the analytic aspects of the problem of linearization. We shall therefore have to make an assumption analogous to (i): An element T of T^k will be called a contraction if the eigenvalues, $s_1, s_2, \cdots, s_m$, of $J(T)$ satisfy

$$(I) \qquad |s_i| < 1.$$

In all the cases we shall treat, we assume, for simplicity that the matrix

$J(T)$ has no multiple elementary divisors. Hence, in the coordinate system corresponding to the eigenvectors of $J(T)$, (I) takes the form

$$\text{(I*)} \qquad \| J(T) \| < 1,$$

where the norm is the ordinary Euclidean norm: $\| J(T) \| = \sup \| J(T) \cdot (x) \|$ where the sup is taken over all vectors (x) such that $\| (x) \| = 1$, with $\| (x) \| = \sum x_i^2$ if x_i are the coordinates of (x) in this coordinate system. If S and s denote $\max s_i$ and $\min s_i$ respectively, then

$$\text{(I**)} \qquad s \| (x) \| < \| J(T)(x) \| < S \| (x) \|.$$

Then we have

Theorem 2. *Let T be a transformation in T^k satisfying* (I) *and* (II) *and such that*

$$(18) \qquad k > \log s / \log S,$$

then there exists a transformation R in T^k such that RTR^{-1} is linear.

In proving this theorem we shall use the method described in [10]. That is, denoting by L the linear transformation which is given by the Jacobian matrix $J(T)$ at the origin, we wish to find an R such that $RTR^{-1} = L$. We rewrite this equation as

$$(19) \qquad R = L^{-1} R T.$$

We shall solve (19) by a process of successive approximations. This process will converge provided that we are able to start with an initial R which satisfies (19) up to terms of sufficiently high order. Such an R will be supplied by Lemma 1. In order to formulate the convergence proof, it is convenient to introduce the following notation. Let $V^k{}_N$ denote the space of n-tuplets $f = (f^1, \cdots, f^n)$ of functions of n real variables defined in some neighborhood N of the origin, which are of class C^k there and which vanish at the origin together with all partial derivatives of order $\leqq k$. Thus $V^j{}_{N'} \subseteq V^k{}_N$ for $N' \supseteq N$ and $j \geqq k$. On the space $V^k{}_N$ we introduce the metric

$$(20) \qquad \| f \|^k{}_N = \sup_N \sum_{i=1}^{n} \sum_{i_j=1}^{n} (f^i{}_{x_{i_1} \cdots x_{i_n}})^2.$$

Then an immediate consequence of the above definitions is

Lemma 2. *Given any f in $V^k{}_N$ and any positive number ϵ, we can find a sufficiently small neighborhood N^ϵ such that*

$$(21) \qquad \| f \|^1{}_{N^\epsilon} + \| f \|^2{}_{N^\epsilon} + \cdots + \| f \|^{k-1}{}_{N^\epsilon} < \epsilon \| f \|^k{}_{N^\epsilon}.$$

Now define the operator $\mathfrak{D}_T$ on $V^k{}_N$ by

$$\mathfrak{D}_T\colon f(\cdot) \to J(T)^{-1}f(T(\cdot)) \tag{22}$$

The essence of the convergence proof is then contained in

LEMMA 3. *Let f be in $V^k{}_N$ and T in T^k with k satisfying* (18). *Then there exists a neighborhood N' of the origin such that*

$$\| \mathfrak{D}_T f \|^k{}_{N'} < K \| f \|^k{}_{N'} \tag{23}$$

for some $K < 1$.

If we call $(t^i{}_j(x))$ the Jacobian matrix of the transformation T at the point x, then for any function f of class C^k on N

$$[f(T(x))]_{x_{j_1}\cdots x_{j_k}} = \sum f_{x_{j_1}\cdots x_{j_k}}(T(x))\, t^{j_1}{}_{i_1}(x) \cdots t^{j_k}{}_{i_k}(x) + P, \tag{24}$$

where P is a polynomial in derivatives of f of order lower than k, and in derivatives of the $t^i{}_j$ (of order $\leqq k$). Since T is smooth near the origin (I**) implies that we can choose N^δ so that $\| (t^i{}_j(x) \| < S + \delta$ for all x in N_δ. If M denotes the maximum of the derivatives of the $t^i{}_j(x)$ occurring in P for all x in N, set $\gamma = \epsilon/M$. Then by Lemma 2, and (24)

$$\| \mathfrak{D}_T f \|_{N^\gamma \cap N_\delta} < s^{-1}[(S + \delta)^k + \epsilon] \| f \|_{N^\gamma \cap N_\delta}. \tag{25}$$

In view of (18), we can choose δ and ϵ so small that (25) reduces to (23).

In order to complete the proof of Theorem 2 we observe that Lemma 1 implies the existence of an R_0 such that $R_0 - L^{-1}RT$ is in $V^k{}_N$. Then Lemma 3 implies that the sequence of transformations

$$R_n = L^{-n}R_0T^n = \sum_{k=0}^{n-1} \mathfrak{D}_T{}^k(L^{-1}R_0T - R)$$

is uniformly convergent and tends to a transformation R in T^k, which clearly satisfies (19), in some neighborhood N^* of the origin.

It should be remarked that although we have defined R only on some small neighborhood N^*, we can extend the definition to any neighborhood N for which T is defined and for which $T^r(N) \subset N^*$ for some suitably large r. In fact, all we have to do is to replace R by $L^{-r}RT^r$. It should also be noted that the above proof is valid in the real analytic case, where it supplies an analytic change of coordinates R.

6. In the last section we proved that any smooth contraction T (and hence the discrete group T^n generated by T) satisfying certain conditions can be linearized. In this section we show how to pass from the discrete case to that of a continuous one-parameter group. Here there are two smoothness considerations: smoothness of the individual transformations and of their time dependence. In what follows both considerations become trivial in virtue of the general principle enunciated in

LEMMA 4. *Let T_t be a continuous one parameter family of transformations in T^k such that T_n is linear for integral n. Then there exists a transformation R in T^k such that*

$$RT_tR^{-1} = L_t, \tag{26}$$

where L_t is the one-parameter group of linear transformations whose matrices are the Jacobians of T_t at the origin.

In fact set

$$R = \int_0^1 L_{-\alpha}T_\alpha \, d\alpha. \tag{27}$$

Now

$$L_{-t}R = \int_0^1 L_{-\alpha-t}T_\alpha \, d\bar{\alpha} = \int_{-t}^{1-t} L_{-\alpha}T_{\alpha+t} \, d\alpha = \int_{-t}^{0} + \int_0^{1-t}.$$

Then, since $L_{-1}T_1 = \text{identity}$,

$$\int_{-t}^{0} L_{-\alpha}T_{\alpha+t} \, d\alpha = \int_{-t}^{0} L_{-\alpha}(L_{-1}T_1)T_{\alpha+t} \, d\alpha = \int_{1-t}^{1} L_{-\alpha}T_{\alpha+t} \, d\alpha.$$

Thus

$$L_{-t}R = \int_0^1 L_{-\alpha}T_{\alpha+t} \, d\alpha = RT_t$$

or R satisfies (26). It is clear from (27) that R satisfies the smoothness requirements and that $J(R)$ is the identity so that R is in T^k.

Now for any one-parameter group, conditions (I) and (II) are independent of the parameter. If they are satisfied for a group of transformations of class T^k where k satisfies (18) (which is also independent of he parameter), we can first linearize a discrete subgroup by Theorem 1, and then the whole group by Lemma 4. Thus we have proved

THEOREM 3. *Let T_t be a continuous one parameter family of contractions s $(T_{s+t} = T_sT_t)$ which satisfy* (I) *and* (II) *and are of class T^k where k satisfies* (18). *Then there exists a change of coordinates R in T^k which linearizes T_t.*

7. We now translate Theorem 3 into a theorem about differential equations. Consider a system of differential equations (3) where the X_i are functions of class C^k defined in some neighborhood of the origin with $X_i(0,\cdots,0)=0$. Then the existence theorem for ordinary differential equations states that there is unique solution

$$(28) \qquad x_i(t,\xi) \text{ such that } x_i(0,\xi)=\xi_i,$$

where $\xi=(\xi_1,\cdots,\xi_n)$ are the initial points for the motion. We regard (28) as a transformation depending upon the parameter t and wish to calculate its Jacobian $\mathfrak{X}(t,\xi^*)=(x_{i\xi_j})=(x_{i\xi_j}(t,\xi^*))$. This can be done by means of the equation of variation. In fact, taking partial derivatives in (3) gives

$$(29) \qquad d(x_{i\xi_j})/dt=\sum X_{ix_r}x_{r\xi_j}.$$

Denoting by $\mathfrak{F}$ the matrix (X_{ix_j}) we see that $\mathfrak{X}$ satisfies the linear differential equation

$$(30) \qquad d\mathfrak{X}/dt=\mathfrak{F}\mathfrak{X},$$

where the initial conditions ξ^* are to be considered as parameters. Setting $\xi=0$ in (30) yields

$$(31) \qquad J(T_t)=e^{At},$$

where A is the matrix of linear terms of (3) at the origin. But then it is clear that condition (I) and (II) for the flow generated by (3) are equivalent to conditions (i_R) and (ii) for the differential equations, while (18) becomes replaced by

$$(32) \qquad k>\Lambda/\lambda,$$

where $\Lambda=\max|\operatorname{Re}\lambda_i|$ and $\lambda=\min|\operatorname{Re}\lambda_i|$. We have thus proved

THEOREM 4. *Any system of differential equations* (3) *defined in some neighborhood of the origin such that* $X_i(0,\cdots,0)=0$, *satisfying conditions* (i) *and* (ii) *and of class* C^k *where* k *satisfies* (32) *can be linearized by a change of coordinates in* T^k.

For the case of analytic differential equations satisfying the (i) and (ii) we can assert that the change of coordinates is analytic. In this case, by the introduction of a complex time, if necessary, we can reduce (i_R) to (i). We thus obtain

THEOREM 5 (Poincaré). *Any system of analytic differential equations*

(3) *satisfying* (i) *and* (ii) *can be linearized by an analytic change of coordinates.*

8. As was shown in Section 3, if the formal condition (ii) is not satisfied, then a contraction can, in general, not be linearized. We can, nevertheless, ask for some other, nonlinear, normal form. Let us first examine where the proof of Lemma 1 breaks down if (ii) does not hold. In fact, let $s_i = s_1^{m_1}\cdots s_n^{m_n}$ where the m_j are integers such that $\sum m_j > 1$. Then, if we set $(i_1,\cdots,i_n) = (m_1,\cdots,m_n)$ in (17) we obtain $P^i_{m_1\cdots m_n} = 0$. Since $P^i_{m_1\cdots m_n}$ is a polynomial in the lower order $r^j_{j_1\cdots j_n}$ which are already uniquely determined, this might not vanish, so that (16) can not in general be satisfied. We can remedy this situation by including the value of these $P^i_{m_1\cdots m_n}$ into the normal form itself. More precisely,

LEMMA 5. *Let T be an element of F^∞ whose matrix of linear terms has no multiple elementary divisors, with eigenvalues $s_1,\cdots,s_n$. Let M_i denote the collection of n-tuplets $(m_1,\cdots,m_n)$ of positive integers such that*

$$s_i = s_1^{m_1}\cdots s_n^{m_n}. \tag{33}$$

Then there exists a transformation R in F^∞ such that RTR^{-1} has the (complex) form

$$N = (\cdots, s_i x_i + \sum A^i_{m_1\cdots m_n} x_1^{m_1}\cdots x_n^{m_n},\cdots), \tag{34}$$

where the $(m_1,\cdots,m_n)$ are in M^i.

The equation corresponding to (16) is

$$\begin{aligned} s_i[x_i + \textstyle\sum r^i_{i_1\cdots i_n} x_1^{i_1}\cdots x_n^{i_n}] &+ \sum_{M_i} A^i_{m_1\cdots m_n}[x_1 + \textstyle\sum r^1_{i_1\cdots i_n} x_1^{i_1}\cdots x_n^{i_n}]^{m_1} \\ &+ \cdots [x_n + \textstyle\sum r^n_{i_1\cdots i_n} x_1^{i_1}\cdots x_n^{i_n}]^{m_n} \\ &= s_i x_i + \textstyle\sum r^i_{i_1\cdots i_n}(s_1x_1)^{i_1}\cdots(s_nx_n)^{i_n} + \cdots. \end{aligned} \tag{35}$$

If we compare the coefficients of $x_1^{i_1}\cdots x_n^{i_n}$ for $(i_1,\cdots,i_n)$ not in M^i we obtain (17) where the $P^i_{i_1\cdots i_n}$ is a polynomial in those $r^j_{j_1\cdots j_n}$ and $A^i_{m_1\cdots m_n}$ for which $\sum j_k$ and $\sum m_k$ are both $< \sum i_k$. We can then solve (17) for $r^i_{i_1\cdots i_n}$ in terms of known quantities, as before. If $(i_1\cdots i_n)$ is in M^i, then (17) is replaced by

$$s_i r^i_{i_1\cdots i_n} + A^i_{i_1\cdots i_n} = (s_1^{i_1}\cdots s_n^{i_n}) r^i_{i_1\cdots i_n} + P^i_{i_1\cdots i_n}. \tag{36}$$

The coefficients of $r^i_{i_1\cdots i_n}$ in (36) cancel and we can determine that $A^i_{i_1\cdots i_n}$. We then can choose the $r^i_{i_1\cdots i_n}$ arbitrarily and (35) will hold. (If we wish to make the $A^i{}_{m_1\cdots m_n}$ unique, we should make some a priori choice of all such $r^i{}_{i_1\cdots i_n}$, which might arise, e. g., set them all equal to zero.) This proves the lemma.

If we now assume that condition (i) holds, then (ii) can be violated only for those $(m_1, \cdots, m_n)$ such that $\sum m_i < k$ where k is given by (18). Thus, in finding a normal form for arbitrary T satisfying (i) and not (ii) all that is necessary is to show that we can choose coordinates in such a manner that T becomes a transformation given by polynomials of degree k. This can be done by the same method as in the proof of Theorem 2:

THEOREM 6. *Let T be a transformation in T^r where $r \geqq k$ and k satisfies* (18) *where the s_i are the eigenvalues of $J(T)$. Then there is a transformation R in T^r such that*

$$P = RTR^{-1}, \tag{37}$$

where P is a transformation given by polynomials of degree $\leqq k$. In fact we can assume that P is given by the image of T in F^k under the natural homomorphism. We can determine a normal form for T by application of Lemma 5.

Proof. It is easy to see that

$$\| P^{-1}S_1T - P^{-1}S_2T \|^r{}_N < \epsilon \| S_1 - S_2 \|^r{}_N + \| L^{-1}S_1T - L^{-1}S_2T \|^r{}_N \tag{38}$$

for any S_1 and S_2 in T^r. If we take $S_1 = P^{-j-1}RT^{j+1}$ and $S_2 = P^{-j}RT^{-j}$, then $S_1 - S_2$ is an element of $V^r{}_N$ if R is a suitably chosen polynomial transformation (reducing to the identity if $r = k$). Then an application of Lemma 4 implies that the series

$$\sum (P^{-j-1}RT^{j+1} - P^{-j}RT^j) \tag{39}$$

converges, proving the theorem.

In the particular case of an analytic transformation in the plane with real eigenvalues $0 < s < t < 1$ for the Jacobian at the origin, Theorem 6 implies that every such surface transformation can be brought into the normal form

$$\begin{aligned} &x^1 = sx + Ay^m, \qquad y' = ty \quad (\text{if } s = t^m) \\ \text{or}\quad &x^1 = sx \qquad\qquad , \qquad y' = ty \quad (\text{if } s \neq t^m \text{ for any } m) \end{aligned} \tag{40}$$

by an analytic change of coordinates; this result was obtained by Lattès [3].

9. In this section we shall consider what happens if (i) is violated. We can not obtain anything approaching a normal form for these transformations, but we shall, nevertheless, outline the proof of a result which is a strong generalization of Theorems 2-6. In what follows, we shall assume for simplicity that all the eignevalues of the Jacobian matrices are real. The transition to the case of non-real eignevalues does not imply any essentially new ideas.

THEOREM 7. *Let T be a transformation in T^k of the form*

$$x^1_i = s_i x_i + g_i(x_1, \cdots, x_n), \tag{41}$$

where the g_i are terms of higher order and

$$| s_i | < 1 \text{ for } i \leqq p, \qquad | s_i | \geqq 1 \text{ for } i > p. \tag{42}$$

Suppose, furthermore that

$$s_j \neq s_1^{m_1} \cdots s_p^{m_p} \qquad (j = 1, 2, \cdots, p) \tag{43}$$

for any positive integers m_i such that $\sum_1^p m_i > 1$, and that k satisfies (18) *where S and s are now defined by*

$$S = \max(| s_1 |, \cdots, | s_p |) \text{ and } s = \min(| s_1 |, \cdots, | s_p |), \tag{44}$$

Then there exists a change of coordinates R in T^k of the particular form

$$y_i = x_i - \phi(x_1, \cdots, x_p) \tag{45}$$

which transforms T into the form

$$y'_i = s_i y_i + G_i(y_1, \cdots, y_n), \tag{46}$$

where the G_i satisfy

$$G_i(y_1, \cdots, y_p, 0, \cdots, 0) = 0 \tag{47}$$

for all i.

It is clear that Theorem 2 is contained in Theorem 6. (Take $p = n$) If we do not assume (43) we have

THEOREM 8. *Let T be a transformation in T^k of the form* (41) *satisfying* (42) *and* (18). *Then there exists a change of coordinates R in T^k of the form* (45) *transforming T into the form* (47) *where $G_i(y_1, \cdots, y_p, 0, \cdots, 0)$ is a polynomial of degree $[\log s / \log S] + 1$ for $i \leqq p$ and*

$$G_i(y_1, \cdots, y_p, 0, \cdots, 0) = 0 \textit{ for } i > p. \tag{48}$$

It is clear that Theorem 7 follows from Theorem 8 via Lemma 1 so that it suffices to prove Theorem 8. It should be remarked that Theorem 8 implies that the surface $y_{p+1} = \cdots y_n = 0$ remains invariant. A more general formulation of this result which does not make use of the somewhat restrictive smoothness assumption (18) and (44) is contained in

THEOREM 9. *Let T be a transformation in T^k of the form* (41) *where the S_i satisfy* (42). *Then there exists a change of coordinates R in T^k of the form*

$$(49) \qquad y_i = x_i, \quad (i \leqq p); \qquad y_i = x_i - \phi_i(x_1, \cdots, x_p) \quad (i > p)$$

which transforms T into the form (46) *where the G_i satisfy* (48).

If we apply Theorem 6 to the invariant surface $y_{p+1} = \cdots y_n = 0$ (assuming that T satisfies the additional smoothness assumption (44)) then Theorem 8 follows from Theorem 9. If q of the eigenvalues s_i are greater than one then applying Theorem 9 to T^{-1} we obtain

THEOREM 10. *Let T be a transformation in T^k of the form* (41) *where p of the s_i are < 1 and q of the s_i are > 1. Then there exist invariant surfaces of class C^k passing through the origin of dimensions $n - p$ and $n - q$.*

Theorem 10 is a complete generaliaztion (to n-dimensions and the non-analytic case) of the result of Poincaré concerning the existence of invariant curves near a hyperbolic point of a surface transformation, cf. [6], pp. 202-204, [2] and [8]. In the case of surface transformations $n = 2$, $p = q = 1$.

If we make use of a slight modification of Lemma 4 and of the remarks before Theorem 5 we can translate Theorem 7 into a theorem about differential equations.

THEOREM 11. *Consider a system of differential equations of the form*

$$(50) \qquad dx_i/dt = \lambda_i x_i + g_i(x_1, \cdots, x_n),$$

where the λ_i satisfy

$$(51) \qquad \lambda_i < 0 \text{ for } i \leqq p,$$

and the g_i are of class C^k where

$$(52) \qquad k > \max_{i \leqq p} |\lambda_i| / \min_{i \leqq p} |\lambda_i|.$$

Then there exists a change of coordinates of the form (45) *transforming* (50) *into the form*

$$(53) \qquad dy_i/dt = \lambda_i y_i + G_i(x_1, \cdots, x_n),$$

where the G_i satisfy (48).

This is a generalization to the non-analytic case of a theorem of Liapounoff [4]. If we similarly translate Theorems 9 and 10 into theorems about differential equations we obtain the 'Asymptotische Bahnen' of Siegel [7] (without his analyticity assumptions).

We have seen that all the results of this section hinge upon Theorem 9. We now proceed to its proof.

Denote by E the projection

$$E: (x_1, \cdots, x_n) \to (x_1, \cdots, x_p, 0, \cdots, 0). \tag{54}$$

Then we rephrase the conclusion of Theorem 9 as follows: there exists an R in T^k of the form (49) such that

$$(RTR^{-1})ER = E(RTR^{-1})ER. \tag{55}$$

We first remark that any transformation R of type (49) is uniquely determined by RE. Furthermore, if a sequence R_n of transformation of the type (49) has the property that R_nE_n converges uniformly along with partial derivatives of a certain order then the sequence R_n has this same property. Finally R^{-1} has the same form as R with the exception that the ϕ_i are replaced by $-\phi_i$. If we translate equation (55) into a functional equation for the ϕ_i we obtain

$$\begin{aligned} s_i\phi_i + g_i[x_1, \cdots, x_p, \phi_{p+1}(x_1, \cdots, x_p) \cdots \phi_n(x_1, \cdots, x_p)] \\ = \phi_i(s_ix_1 + g_1[x_1, \cdots, x_p, \phi_{p+1}(x_1, \cdots, x_p), \cdots], \\ \cdots s_px_p + g_p[x_1, \cdots, x_p, \phi_{p+1}(x_1, \cdots, x_p), \cdots]) \end{aligned} \tag{56}$$

for $i = p + 1, \cdots, n$. We write this equation as

$$\begin{aligned} \phi_i = s_i^{-1}\{\phi_i(s_1x_1 + g_1[x_1, \cdots, x_p, \phi_{p+1}, \cdots, \phi_n], \\ \cdots s_px_p + g_p[x_1, \cdots, x_p, \phi_{p+1}(x_1, \cdots, x_p), \cdots]) \\ - g_i[x_1, \cdots, x_p, \phi_{p+1}, \cdots, \phi_n]\}. \end{aligned} \tag{57}$$

We now observe that all the s_j occurring inside the functions in (57) are strictly less than one, while the s_i^{-1} occurring as factors are less than or equal to one as a consequence of (42) and (49). Furthermore the g's occurring in (57) are functions of second order. Applying Taylor's theorem twice, we can, therefore, solve (57) by an iteratuve procedure similar to that used in the proofs of Theorems 2 and 6.

NEW YORK UNIVERSITY.

REFERENCES.

[1] G. D. Birkhoff, *Dynamical Systems*, American Mathematical Society Colloquium Publication, Number 9.

[2] J. Hadamard, *Selecta*, 1901, pp. 163-166.

[3] S. Lattès, *Comptes Rendus*, vol. 152 (1911), pp. 1566-1569.

[4] A. Liapounoff, *Problème générale de la stabilité du mouvement*, Annals of Mathematics Studies, Number 17.

[5] E. Picard, *Traité d'Analyse*, vol. 3.

[6] H. Poincaré, *Oeuvres*, vol. 1.

[7] C. L. Siegel, "Der Dreierstoss," *Annals of Mathematics*, vol. 42 (1941), pp. 156-162.

[8] S. Sternberg, "On the behaviour of invariant curves near a hyperbolic point of a surface transformation," *American Journal of Mathematics*, vol. 75 (1955), pp. 526-534.

[9] S. Sternberg, "On local C^n contractions of the real line," *Duke Mathematical Journal*, vol. 24 (1957), pp. 97-102.

[10] S. Sternberg and P. Ungar, "On a class of functional equations," to appear.

COVERINGS OF ALGEBRAIC CURVES.*

By Shreeram Abhyankar.

1. Introduction. In this paper we present, among other things, some new results concerning coverings of algebraic curves—i. e., in global ramification theory—which distinguish the modular case from the classical, i. e., the characteristic zero case, and seems to open up new lines of research. Throughout the paper several problems will be formulated and questions raised.

We had noted in [A1] that the possibility of "local splitting of a simple branch variety by itself" is the basic fact underlying the difference between local ramification theory in the modular and the classical cases. One thesis of this paper is that the corresponding global possibility of the "splitting of a single branch point by itself" is the basic fact which distinguishes the global ramification theory in the modular case from that in the classical case. For instance, the following three are some of the consequences of this *possibilty*; let the ground field k be algebraically closed of characteristic $p \neq 0$: (1) Given any one-dimensional algebraic function field K/k there exists x in K (not in k) such that $x = \infty$ is the only valuation of $k(x)/k$ ramified in K, i. e., the total differential dx has no zero or pole at finite distance (Theorem 4 of Section 2). [Hasse and Deuring had proved that for each $p \neq 2$ there exist finite number of elliptic function fields of this type.] (2) There exist unsolvable unramified coverings of the affine line—which is a commutative group variety (Section 4). (3) For nontamely ramified extensions, in no possible sense is the monodromy group generated by loops around the branch points (Remark 7 of Section 4). (1) leads to the concept of universal branch loci and the possibility of new invariants. (2) is only a very special consequence of a general pattern which leads us to formulate a conjecture which roughly says that: (ramification theory in characteristic $p \neq 0$) = (ramification theory in characteristic zero for the *corresponding* situation) + (the class of all quasi p-groups[1]); for the local theory some evidence for this conjecture is in our previous papers [A1] and [A3] and some evidence for the global theory for curves is given in this

---

* Received February 8, 1957.

[1] As defined in [A3], for a given prime number p, a finite group G is said to be a quasi p-group if G is generated by its p-sylow subgroups.

paper (Section 4). This conjecture consists mainly of two parts: the first part asks us to algebraize the fundamental group in the classical case and carry it over to tamely ramified extensions, for this and other comparative purposes we have collected in Section 7 information on the topological fundamental and monodromy groups in the classical case for curves; the second part of the conjecture says that if (for characteristic $p \neq 0$) in a situation, nontrivial coverings are possible, then coverings exist with any assigned quasi p-group.

The recent result of Lang-Serre to the effect that for a curve there are only a finite number of unramified coverings of a given degree is generalized in Section 6 to tamely ramified extensions with assigned branch points. In Section 5 is given a formula to derive from the different of an extension the different of the corresponding least galois extension. In the Appendix (Section 8) are collected some lemmas used in the paper. The contents of the other sections should be clear from their titles; the reader who wants a quick look at the amusing results is referred to Section 4.

Notations. All through the paper we shall tacitly use the notations and results of [A1] and Section 2 of [A2]. Now let t be a power series in $X, Y, \cdots$ with $X = (X_1, X_2, \cdots, X_a)$, $Y = (Y_1, Y_2, \cdots, Y_b) \cdots$ having coefficients in a field k; we shall use the following notations:

$$| t |_X = \text{leading degree of } t \text{ in } X;$$

$$| t |_{X,Y} = \text{leading degree of } t \text{ in } X \text{ and } Y; \text{ etc.}$$

If t is a polynomial in X (in X and Y; etc.) then:

$$\| t \|_X = \text{the degree of } t \text{ in } X;$$

$$\| t \|_{X,Y} = \text{the degree of } t \text{ in } X \text{ and } Y; \text{ etc.}$$

When the reference to X (or X, Y) is clear from the context, we may omit these subscripts. Note that: $| 0 | = \infty$ and $\| 0 \| = -\infty$. For a polynomial $F(Z)$ we shall denote by $DF(Z)$ the Z-discriminant of $F(Z)$.

Now let K/k be an n-dimensional algebraic function field and let K^* be a finite separable extension of K. Let V be a normal projective model of K/k, let V^* be a K^*-normalization of V. Let W be an irreducible subvariety of V and let $W^*_1, \cdots, W^*_s$ be the irreducible subvarieties of V^* corresponding to W; let R and R^*_i be the quotient rings of W and W^*_i on V and V^* respectively; let w be a real discrete valuation of K and let $w^*_1, \cdots, w^*_t$ be the K^*-extension of w. We shall say that respectively $W^*_1/W, R^*_1/R, w^*_1/w$ are *tamely ramified* if in case $p \neq 0$ we have $r(W^*_1 : W)$,

$r(R_1:R)$, $r(w^*_1:w) \not\equiv 0 \pmod{p}$ respectively. We shall say that respectively W, R, w are *tamely ramified in* K^* if respectively W^*_i/W, R^*_i/R, w^*_i/w are tamely ramified for all i. We shall say that V is tamely ramified in K^* (and K^* or V^* is tamely ramified over V) if each irreducible subvariety of W is tamely ramified in K^*. Observe that for $n=1$, V^* is tamely ramified over V if and only if each valuation of K/k is tamely ramified in K^*; in this case we shall say that K^*/K (or K in K^*) is tamely ramified.

2. Splitting of a single branch point by itself. Let k be an arbitrary field of characteristic $p \neq 0$. In [A1, Remark in Section 2] we had noted that the possibility of "local splitting of a simple branch variety by itself" is the basic fact underlying the difference between the structures of local galois groups in the case of nonzero characteristic and in the case of zero characteristic. This possibility was exhibited by the normal surface S^* [Example 5 of A1]: $Z^{p+1}+Y^{p-1}+X^{p+1}=0$, for the Z-projection of S^* onto the X,Y plane S the branch locus is $D: X=0$. Now we shall exploit this surface, or rather its section by the plane $Y=X$, for global ramification theory and the corersponding conclusion will be that the possibility of "global splitting of a (single) branch point by itself" is the basic fact underlying the difference between the global ramification theories in the case of nonzero characteristic and in the case of zero characteristic.

So consider the polynomial

$$F(Z)=Z^{p+1}+x^{p-1}+x^{p+1}\in k[x][Z],$$

where x is a transcendental over k. Let $Z=Z^*x^2$ and $F^*(Z^*)=x^{-p-1}F(Z)$, so that

$$\begin{aligned} F^*(Z^*) &= x^{-p-1}[(x^2Z^*)^{p+1}+x^{p-1}(x^2Z^*)+x^{p+1}] \\ &= x^{p+1}Z^{*p+1}+Z^*+1\equiv 1(Z^*+1)\ [\operatorname{mod} x]. \end{aligned}$$

Hence by Hensel's lemma [for instance Lemma 1 on page 43 of C]: $F^*(Z^*)=G^*(Z^*)(Z^*+u)$ where $u\in k[[x]]$ with $u(0)=1$ and $G^*(Z^*)$ is of degree p in Z^* with $G^*(Z^*)\equiv 1\ [\operatorname{mod} x]$. Therefore

$$F(Z)=G(Z)(Z+ux^2),$$

where

$$G(Z)=Z^p+G_1Z^{p-1}+G_2Z^{p-2}+\cdots+G_p, \qquad G_i\in k[[x]].$$

Then

$$\begin{aligned} F(Z) &= Z^{p+1}+(G_1+ux^2)Z^p+(G_2+ux^2G_1)Z^{p-1}+\cdots \\ &\quad +(G_{i+1}+ux^2G_i)Z^{p-i}+\cdots+(G_p+ux^2G_{p-1})Z+ux^2G_p. \end{aligned}$$

Hence

(1) $$G_1+ux^2=G_2+ux^2G_1=\cdots=G_{p-1}+ux^2G_{p-2}=0$$

(2) $$G_p+ux^2G_{p-1}=x^{p-1}$$

and

(3) $$ux^2G_p=x^{p+1}.$$

Now (1) implies that

$$G_1=-ux^2,\quad G_2=-ux^2G_1,\quad G_3=-ux^2G_2,\cdots,G_p=-ux^2G_{p-2},$$

so that

(4) $$G_1=-ux^2,\quad G_2=u^2x^4,\quad G_3=-u^3x^6,\cdots,G_i=(-1)^iu^ix^{2i},\cdots,G_{p-1}=(-1)^{p-1}u^{p-1}x^{2(p-1)},$$

i.e., $G_{p-1}=u^{p-1}x^{2p-2}$. Hence by (2) we have

(5) $$G_p=x^{p-1}-ux^2G_{p-1}=x^{p-1}-u^px^{2p}=x^{p-1}(1-u^px^{p+1}).$$

Since $u(0)=1$, $|u|=0$. Hence by (4) and (5) we have:

(6) $$|G_i|=2i \text{ for } i=1,2,\cdots,p-1 \text{ and } |G_p|=p-1.$$

Therefore by Lemma A1 (of Section 8) $G(Z)$ is irreducible in $k[[x]][Z]$. Let v be the valuation of $k((x))/k$ given by x, let z be a root of $G(Z)$, w be the unique extension of v to $k((x))(z)$. Then [O, Theorem II on page 298] $w(z)=(1/p)w(G_{p-1})=[(p-1)/p]w(x)$. Therefore $\bar{r}(w:v)$ is divisible by p and hence $\bar{r}(w:v)=p$ and (the residue field of w) $=$ (the residue field of v) $=k$. Thus

(7) $$F(Z)=G(Z)(X+ux^2),\ G(Z) \text{ irreducible in } k[[x]][Z].$$

Hence if $F(Z)$ were reducible in $k[x][Z]$ it must have $Z+u^*$ as a factor with $u^*=ux^2\in k[x]$. Then

$$0=F(-u^*)=u^{*p+1}-x^{p-1}u^*+x^{p+1}.$$

Hence the x-degrees of two of the three terms u^{*p+1}, $x^{p-1}u^*$, x^{p+1} must be equal. Now $\|u^{*p+1}\|\geqq|u^{*p+1}|=2(p+1)>p+1=\|x^{p+1}\|$; and $\|u^{*p+1}\|=\|x^{p-1}u^*\|$ implies $\|u^{*p}\|=\|x^{p-1}\|=p-1$, i.e., $\|u^*\|=(p-1)/p=$ a noninteger which is a contradiction. Therefore $\|x^{p-1}u^*\|=\|x^{p+1}\|$, i.e., $\|u^*\|=2$. Since $|u^*|=2$ we must have $u^*=cx^2$ with $0\neq c\in k$. Now $F(-cx^2)=c^{p+1}x^{2p+2}-cx^{p+1}+x^{p+1}$ so that $\|F(-cx^2)\|=2p+2$ which is a contradiction since $F(-cx^2)=0$.

Thus $F(Z)$ is irreducible in $k[x][Z]$ and hence in $k(x)[Z]$ and $F(Z)$

factors in $k[[x]][Z]$ i.e., in $k((x))[Z]$ into two irreducible factors of degrees p and 1 respectively and these factors do not introduce any residue field extensions.

[*Remark* 1. It would be interesting to compute the galois group of $F(Z)$ over $k((x))$, i.e., (assuming k to be algebraically closed) by Lemma A2 (of Section 8) the galois group of $Z^p + x^2Z^{p-1} + x^{p-1}$ over $k((x))$; that ought to yield the galois group of $F(Z)$ over $k(x)$.]

Let $K = k(x)$, let z be a root of $F(Z)$ and let $K^* = K(z)$. Let C be the irreducible curve: $Z^{p+1} + X^{p-1}Z + X^{p+1} = 0$ in the X, Z plane and let L be the X axis. Then $K = k(L)$, $K^* = k(C)$ and the rational map given by the embedding $K \subset K^*$ corresponds to the projection of C (by lines parallel to the Z-axis) onto L. Now $F'(Z) = Z^p + x^{p-1}$ so that $F(Z) = ZF'(Z) + x^{p+1}$ and hence $DF(Z) = x^{p(p+1)}$. Therefore the origin, i.e., the valuation v given by the irreducible nonunit x of $k[x]$, is the only possible branch point on L at finite distance. To test for the point at infinity let $x_1 = 1/x$, $Z_1 = Zx_1$ and $F_1(Z_1) = x_1^{p+1}F(Z)$ so that

$$F_1(Z_1) = x_1^{p+1}(x_1^{-p-1}Z_1^{p+1} + x_1^{-p+1}x_1^{-1}Z_1 + x_1^{-p-1}) = Z_1^{p+1} + x_1Z_1 + 1.$$

Now $F'_1(Z_1) = Z_1^p + x_1$ so that $F_1(Z_1) = Z_1F'_1 + 1$ and hence $DF_1(Z_1) = 1$. Therefore the point at infinity is not ramified. Thus the origin of L is the only possible branch point. From the way $F(Z)$ factors in $k((x))[Z]$ we conclude that v splits in K^* into two valuations w_1 and w_2 both of which are rational over k with $\bar{r}(w_1 : v) = d(w_1 : w) = p$ and $\bar{r}(w_2 : v) = d(w_2 : v) = 1$. Now the curve C is of degree $p + 1$ and it has a p-fold point at the origin. Therefore C is rational (over k), i.e., there exists y in K^* such that $K^* = k(y)$, since w_1 and w_2 are rational over k we may assume that they correspond to $y = 0$ and $y = \infty$ respectively (Lemma A3 of Section 8).

[If k is algebraically closed and if we were willing to deal with a generic section of S we could *perhaps* argue thus (and in fact this is how we were led to the construction we have just given): Let $L : aX + bY = 0$ $(a, b \in k)$ be a *generic* line in the X, Y plane S; then the curve C on the surface S^* which corresponds to L is irreducible; C is the intersection of S^* with the *plane* $aX + bY = 0$ in the X, Y, Z space; for the induced rational map of C onto L the branch locus $\bar{D}$ is the intersection of L with D, i.e., $\bar{D}$ is a single point and since $[k(C) : k(L)] = p + 1$ it follows by Proposition 6 (Section 3) that $\bar{D}$ splits in $k(C)$ into two points with ramification indices p and 1 respectively.]

To find y explicitly we may proceed as follows. Homogenizing

$Z^{p+1} + X^{p-1}Z + X^{p+1} = 0$ we get $Z^{p+1} + X^{p-1}YZ + X^{p+1} = 0$. Thus the p-fold singularity of C is: $X = 0$, $Y = 1$, $Z = 0$. Take $X = 0$ to be the line at infinity. Let $x' = Y/X$ and $y = Z/X$; previously we had $x = X/Y$ and $z = Z/Y$, i.e., $y = z/x$ and $x' = 1/x$, i.e., $z = y/x'$ and $x = 1/x'$ so that $(y/x')^{p+1} + (1/x'^{p-1})y + (1/x'^{p+1}) = 0$, i.e., $y^{p+1} + x'y + 1 = 0$. Hence $1/x = x' = (-1 - y^{p+1})/y = -(1/y) - y^p$. Now $x = 0$ if and only if $x' = \infty$. Replace x by $(-x')$. Then $y^{p+1} - xy + 1 = 0$, so that $x = y^p + y^{-1}$, $x = \infty$ is the only branch point in $k(x)/k$ for $k(y)$ and on it lie $y = 0$ and $y = \infty$. If we replace y by y^{-1} then $y^{p+1} - xy^p + 1 = 0$, $x = y + y^{-p}$, $x = \infty$ is the only branch point and on it lie $y = 0$ and $y = \infty$. Thus we may state and directly reprove

THEOREM 1. *Let $k(y)$ be a simple transcendental extension of an arbitrary ground field k of characteristic $p \neq 0$. Let $x = y + y^{-p}$. Then (1) $[k(y) : k(x)] = p + 1$; (2) v: $x = \infty$ is the only valuation of $k(x)/k$ which is ramified in $k(y)$; (3) v splits in $k(y)$ in the valuations w_0: $y = 0$ and w_∞: $y = \infty$; and (4) $d(w_0 : v) = p$ and $d(w_\infty : v) = 1$.*

Proof. $x = y + y^{-p} = (y^{p+1} + 1)/y^p$; since the numerator and denominator are coprime we have $[k(y) : k(x)] = p + 1$ and $y^{p+1} + xy^p + 1 = 0$ is the minimal equation of y over $k(x)$ [see § 63 of V] i.e., $F(X) = Z^{p+1} + xZ^p + 1$ is the minimal monic polynomial of y over $k(x)$. Now $F'(Z) = Z^p$ so that $DF(Z) = 1$ and hence no valuation of $k(x)/k$ except possibly v is ramified in $k(y)$. Also the equation $x = y + y^{-p}$ implies that if w is a valuation of $k(y)/k$ with $w \neq w_0$ and $w \neq w_\infty$ then $w(x) \geqq \min[w(y), w(y^{-p})] = 0$ and hence w_0 and w_∞ are the only valuations of $k(y)/k$ which can possibly lie over v. Since $1/x = y^p/(y^{p+1} + 1)$, $w_0(1/x) = p$ and hence w_0 does lie over v and $d(w_0 : v) = \bar{r}(w_0 : v) = p$. Again

$$(1/x) = y^p/(y^{p+1} + 1) = [y^{-p-1}y^p]/[y^{-p-1}(y^{p+1} + 1)] = y^{-1}/(1 + y^{-p-1})$$

so that $w_\infty(1/x) = w_\infty(y^{-1}) - w_\infty(1 + y^{-p-1}) = 1$ and hence w_∞ does lie over v and $d(w_\infty : v) = \bar{r}(w_\infty : v) = 1$. [Check:

$$p + 1 = [k(y) : k(x)] = \textstyle\sum_{w \text{ over } v} d(w : v) = d(w_0 : v) + d(w_\infty : v) = p + 1.]$$

THEOREM 2. *Let $k(y)$ be a simple transcendental extension of an arbitrary ground field k of characteristic $p \neq 0$. Let $w_1, w_2, \cdots, w_n$ be a finite set of given valuations of $k(y)/k$ which are rational over k, i.e., we are given a finite set of distinct elements $c_1, c_2, \cdots, c_n$ in $k \cup \{\infty\}$ such that c_i is the residue of y at w_i. Then there exists x in $k(y)$ (not in k) such that v: $x = \infty$ is the only valuation of $k(x)/k$ which is ramified in $k(y)$ and $w_1, w_2, \cdots, w_n$ lie above v.*

Proof. It is enough to prove that there exists a subfield K of $k(y)$ such that K is a simple transcendental extension of k such that $w_1, w_2, \cdots, w_n$ contract in K to a single caluation v and v is the only valuation of K/k ramified in $k(y)$; for then the rationality of w_1/k implies the rationality of v/k and by Lemma A3 of Section 8 we may find a generator x of K/k such that v corresponds to $x = \infty$. Now we shall make induction on n: for $n = 1$, we may take $K = k(y)$, so let $n > 1$ and assume the theorem for $n - 1$. Then by the induction hypothesis there exists a simple transcendental extension L of k contained in $k(y)$ such that $w_1, w_2, \cdots, w_{n-1}$ contract in L to a single valuation u_0 and u_0 is the only valuation of L ramified in $k(y)$. Let u_∞ be the contraction of w_n to L. If $u_0 = u_\infty$ we may take $K = L$, so now assume that $u_0 \neq u_\infty$. By Lemma A3 of Section 8 we can find a generator y' of L/k such that u_0 is $y' = 0$ and u_∞ is $y' = \infty$. Applying Theorem 1 to $k(y')/k$ find x in L (not in k) such that v: $x = \infty$ is the only valuation of $k(x)/k$ which is ramified in L and u_0 and u_∞ are exactly the valuations of L lying above v. If we let $K = k(x)$ the induction is complete.

Remark 2. If k is finite, we may take $w_1, w_2, \cdots, w_n$ to be all the rational valuations of $k(y)/k$. Then all the rational points of the y-line will lie on the point at infinity of the x-line so that each finite rational point of the x-line will undergo residue field extensions but no ramification. *Question. How far can we assign these residue field extensions?*

PROPOSITION 1. *Let $k(y)$, w_0 and w_∞ be as in Theorem* 1. *If we take $x = y^t + c_1 y^{-p} + c_2 y^{-2p} + \cdots + c_h y^{-hp}$ with $c_1, c_2, \cdots, c_h$ in k, $c_h \neq 0$, $t > 0$ with $t \not\equiv 0 \pmod{p}$, then* (1) $[k(y):k(x)] = hp + t$; (2) v: $x = \infty$ *is the only valuation of $k(x)/k$ which is ramified in $k(y)$; v splits in $k(y)$ into w_0 and w_∞; and* (4) $d(w_0:v) = hp$ *and* $d(w_\infty:v) = t$.

Proof. This is similar to the proof of Theorem 1.

PROPOSITION 2. *Let $k(y)$ and $w = w_\infty$ be as in Theorem* 1. *If we take $x = c_0 y + c_1 y^p + \cdots + c_{m-1} y^{(m-1)p} + y^{mp}$ with $c_0, c_1, \cdots, c_{m-1}$ in k and $c_0 \neq 0$ then* (1) $[k(y):k(x)] = mp$; (2) v: $x = \infty$ *is the only valuation of $k(x)/k$ which is ramified in $k(y)$; and* (3) *w is the only valuation of $k(y)$ lying above v [so that $d(w:v) = \bar{r}(w:v) = mp$].*

Proof. Now $F(Z) = Z^{mp} + c_{m-1} Z^{(m-1)p} + \cdots + c_1 Z^p + c_0 Z - x$ is the minimal monic polynomial of y over $k(x)$; $F'(Z) = c_0$ and hence $DF(Z) = c_0{}^{mp}$ so that v: $x = \infty$ is the only valuation of $k(x)/k$ which can possibly be ramified in $k(y)$. Let w^* be a valuation of $k(y)/k$. Then from the equation defining x it is clear that $w^*(y) \geqq 0$ if and only if $w^*(x) \geqq 0$ and hence $w: y = \infty$ is the only valuation of $k(y)$ lying above $v: x = \infty$.

We may strengthen Theorem 2 thus:

THEOREM 3. *Let the notation be as in Theorem* 2. *By Lemma* A3 *of Section* 8 *we may assume that* $c_1 = \infty$. *Assume* $n > 1$ *and let* $m_2, m_3, \cdots, m_n$ *be arbitrary positive integers which are divisible by* p *and let* $m_1 = 1$. *Let* $x = y + (y - c_2)^{-m_2}(y - c_3)^{-m_3} \cdots (y - c_n)^{-m_n}$. *Then* (1) $[k(y):k(x)] = m_1 + m_2 + \cdots + m_n$; (2) $v: x = \infty$ *is the only valuation of* $k(x)/k$ *which is ramified in* $k(y)$; (3) $w_1, w_2, \cdots, w_n$ *are exactly the valuations of* $k(y)$ *which lie above* v; *and* (4) $d(w_i:v) = \bar{r}(w_i:v) = m_i$ *for* $i = 1, 2, \cdots, n$.

Proof. This is similar to the proof of Theorem 1.

Remark 3. In reference to Theorem 3, by Proposition 6 (Section 3) we know that at least one of the m_i is divisible by p. However, in Theorem 3 we have assumed that $m_1 = 1$ and the other m_i are divisible by p; invoking Proposition 2 before applying Theorem 3, we may take m_1 also to be an arbitrary integer divisible by p. *Question. How far can the assumptions on the* m_i *be relaxed?*

Given $w_1, \cdots, w_n$ and $m_1, \cdots, m_n$ determine all x—or rather $k(x)$—of the type described in Theorem 3 or rather determine all possible structures of $k(y)/k(x)$. Now reverse the problem: i. e., suppose $k(x)$, v and $m_1, \cdots, m_n$ are given. Find all finite algebraic extensions K^* of $K = k(x)$ [to begin with those K^* which are simple transcendental extensions of k and then others as well] such that v is the only valuation of $k(x)/k$ which is ramified in K^*, there are n valuations $w_1, \cdots, w_n$ of K^*/k lying above v and $d(w_i:v) = m_i$ for $i = 1, \cdots, n$. Do this for k algebraically closed and $n = 1$, then $n = 2$ and so on. Is there any smallest value of n which would yield all function fields? Now replace $k(x)$ by an arbitrary one-dimensional function field.

From Theorem 2, we at once derive the following theorem which will be put into its right perspective in Section 4.

THEOREM 4. *Let* K *be a simple transcendental extension of an algebraically closed field* k *of characteristic* $p \neq 0$ *and let* v *be a valuation of* K/k. *Then* (I) *given a one-dimensional algebraic function field* L/k *there exists a finite algebraic extension* L_1 *of* K *such that* L_1 *is* k*-isomorphic to* L *and such that* v *is the only valuation of* K/k *which is possibly ramified in* L. *Also* (II) *given a one-dimensional algebraic function field* L/k *and a finite separable algebraic extension* L^* *of* L *there exists a finite algebraic* *extension* L_1 *of* K *and a finite algebraic extension* L^*_1 *of* L_1 *such that* L^*_1 *is isomorphic to* L^* *under a* k*-isomorphism which maps* L_1 *onto* L *and* v *is the only valuation of* K/k *which is possibly ramified in* L^*_1.

Proof. Taking $L = L^*$, (I) follows from (II), hence it is enough to prove (II). Fix y in L, not in k, and let $K^* = k(y)$. Let $w_1, w_2, \cdots, w_n$ be the valuations of K^*/k which are ramified in L^* (if no valuation of K^*/k is ramified in L^* we may take for $w_1, \cdots, w_n$ any valuations of K^*/k). By Theorem 2 there exists x in K^*, not in k, such that $w_1, \cdots, w_n$ contact in $k(x)$ to a single valuation w and w is the only valuation of $k(x)/k$ which is ramified in K^*. By Lemma A3 of Section 8 there exists a k-isomorphism s of $k(x)$ onto K which maps w onto v; extend s to an isomorphism t of L^* into an algebraic closure of K, let $L^*_1 = t(L^*)$ and $L_1 = t(L)$. Then v is the only valuation of K/k which is possibly ramified in L^*_1.

Remark 4. Part (I) of Theorem 4 may also be stated thus: "Given a one-dimensional algebraic function field L over an algebraically closed ground field k of characteristic $p \neq 0$, there exists x in L not in k such that $x = \infty$ is the only valuation of $k(x)/k$ ramified in L; in other words, the total differential dx has no zeros or poles except at $x = \infty$." An extremely special case of this is known, namely it follows from the work of Hasse [H] and Deuring [D], see also Serre [S], that for each value of $p \neq 2$, there exist a finite number of elliptic function fields L/k for which this is true; of course we prove it for *all* function fields.

3. Coverings of the line with one, two or three branch points. In this section, K denotes a simple transcendental extension of an algebraically closed field k of characteristic p, and S_n denotes the symmetric group on n letters.

PROPOSITION 3. *Let* v_1, v_2, v_3 *be any three distinct valuations of* K/k *and let* n *be a positive integer bigger than one such that either* (I) n, $n-1 \not\equiv 0 \pmod{p}$ *in case* $p \neq 0$, *or* (II) n *is odd and* n, $n-2$, $2 \not\equiv 0 \pmod{p}$ *in case* $p \neq 0$. *Then there exists a finite algebraic extension* L/K *such that* (1) L/k *is a simple transcendental extension,* (2) *for a least normal extension* L^* *of* K *containing* L, *the galois group of* L^*/K *is isomorphic to* S_n, (3) v_1, v_2, v_3 *are exactly the valuations of* K *which are ramified in* L, *i.e., in* L^* (*except when* $n = 2$ *in which case only* v_1 *and* v_2 *are ramified*), *and* (4) K *is tamely ramified in* L *and hence* (*by Proposition 7 of Section* 5) *in* L^*.

Proof. Let $L = k(y)$ be a simple transcendental extension of k, let $x = y^{n-1}(y-1)$ and $f(Z) = Z^{n-1}(Z-1) - x$ in case (I) and let $x = y^{n-2}(y-1)^2$ and $f(Z) = Z^{n-2}(Z-1)^2 - x$ in case (II). Then $[L:k(x)] = n$ and $f(Z)$ is the minimal monic polynomial of y over $k(x)$ [§ 63 of V], and in view of Lemma A3 of Section 8 it is enough to prove that there are exactly three valuations of $k(x)/k$ which are ramified in L and $f(Z)$ is unaffected over $k(x)$, i.e., the galois group of $f(Z)$ over $k(x)$ is S_n. Let w_0, w_1, w_∞ be the valuations of $k(y)/k$ given by $y = 0, 1, \infty$ respectively and let v_0, v_∞ be the valuations of $k(x)/k$ given by $x = 0, \infty$ respectively. It is clear from defining equations of x that $w_\infty(x) = -n$ so that w_∞ lies above v_∞ and $d(w_\infty : v_\infty) = n$ so that w_∞ is the only valuation of $k(y)$ lying above v_∞; also in case (I): $w_0(x) = n-1$, $w_1(x) = 1$, $n-1+1 = n = [k(y):k(x)]$ and in case (II): $w_0(x) = n-2$, $w_1(x) = 2$, $n-2+2 = n = [k(y):k(x)]$, hence in either case w_0 and w_1 are the only valuations of $k(y)$ lying above v_0. Now $(n-1) + [(n-1)-1] = 2n-3 = (n-1) + [(n-2)-1] + [2-1]$ and hence in either case $2n-3$ is the contribution of v_0 and v_∞ to the degree λ of the different of $k(y)$ over $k(x)$. Since both these fields are of genus zero, we have: $-2 = \lambda - 2n$, i.e., $\lambda = 2n-2$ so that $\lambda - (2n-3) = 1$. Hence there is only one more valuation v of $k(x)$ which is ramified in $k(y)$ and only one valuation w of $k(y)$ lying above v is ramified over v and $d(w:v) = 1+1 = 2$ [v will be different in cases I and II; its value can at once be found, by computing $Df(Z)$, to be $x = -n^{-n}(n-1)^{n-1}$ and $x = 4n^{-n}(n-2)^{n-2}$ respectively]. Since $p \neq 2$, $2 \not\equiv 0 \pmod{p}$ and hence it follows [by Section 5 and Lemma A5 of Section 8] that if t is a uniformizing parameter at v then the galois group of $f(Z)$ over $k((t))$ is generated by a 2-cycle and hence the galois group of $f(Z)$ over $k(x)$ contains a 2-cycle. In case (I) the galois group of $f(Z)$ over $k((x))$ is generated by an $(n-1)$-cycle [see Section 5 and Lemma A5 of Section 8] and hence the galois group of $f(Z)$ over $k(x)$ contains an $(n-1)$-cycle and hence it must be S_n [Lemma 1 of A3]. Again in case (II) the galois groups of $f(Z)$ over $k((x))$ and $k((1/x))$ are generated respectively by an n-cycle and by a permutation of type $(1,2)(3,4,\cdots,n)$ so that the galois group of $f(Z)$ over $k(x)$ contains an n-cycle and a permutation of type $(1,2)(3,4,\cdots,n)$ and hence it must be S_n [Lemma 3 of A3].

PROPOSITION 4. *Assume that $p \neq 2$. Let v_1, v_2, v_3 be any three distinct valuations of K/k and let q be any integer. Then there exists a tamely ramified finite algebraic extension L of K such that* (I) *L/k is simply transcendental,* (II) *v_1, v_2, v_3 are exactly the valuations of K/k which are* *ramified in L and* (III) (*the number of valuations of L lying above v_1, v_2, v_3*) $\geqq q+1$.

Proof. By any one of the constructions used in the proof of Proposition 3, there exists a finite algebraic extension K_1 of K such that (I.1) K_1/k is simple transcendental, (II.1) v_1, v_2, v_3 are exactly the valuations of K/k which are ramified in K_1 and (III.1) if by q_1 we denote the number of valuations of K_1 lying above v_1, v_2, v_3 then $q_1 \geqq 3+1$. Replacing K and v_1, v_2, v_3 by K_1 and any three valuations of K_1/k lying above v_1, v_2, v_3 obtain K_2; then from K_2, obtain K_3 and so on; denote by q_n the number of valuations of K_n lying above v_1, v_2, v_3. Then $q_n \geqq 3+n$ and hence it is enough to take $L = K_q$.

PROPOSITION 5. *Assume $p=2$, let n be any positive integer and let v_1 and v_2 be any two valuations of K/k. Then there exists a galois extension L of K with galois group isomorphic to S_n such that v_1 and v_2 are the only valuations of K/k which are possibly ramified in L.*

Proof. For $n=1$ or 2 the matter being trivial we assume $n>2$. If n is even, let $F(Z) = Z^n + f_1Z^{n-1} + f_2Z^{n-2} + \cdots + f_{n-2}Z^2 + (f_{n-1}+y)Z + f_n$ be any one of the polynomials obtained in Chapter I of [A3]; we may replace $f_{n-1}+y$ by y so that $F(Z) = Z^n + f_1Z^{n-1} + \cdots + f_{n-2}Z^2 + yZ + f_n$ and $DF(Z) = y^n$. If n is odd, let $F(Z) = Z^n + f_1Z^{n-1} + f_2Z^{n-1} + \cdots + f_{n-1}Z + f_n + y$ be any one of the polynomials obtained in Chauter II of [A3]; we may replace $f_n + y$ by y so that $F(Z) = Z^n + f_1Z^{n-1} + f_2Z^{n-2} + \cdots + f_{n-1}Z + y$ and $DF(Z) = y^{n-1}$. Thus in either case we have

$$F(Z) = Z^n + F_1Z^{n-1} + F_2Z^{n-2} + \cdots + F_n,$$

with $F_i \in k[x,y]$ and $DF(Z) = y^n$ or y^{n-1} according as n is even or odd. Let S be the projective x, y plane over k so that $k(S) = k(x,y) = K^*$ and let S^* be a normalization of S into a root field L^* of $F(Z)$ over K^*. Then the branch locus of S^* over S is contained in the union Δ of the x-axis ($y=0$) and the line at infinity in S and by the results of [A3], the galois group of L^*/K^* is isomorphic to S_n. Let S_1 be a *generic* line (rational over k) in S and let S^*_1 be the curve on S^* corresponding to S_1. Then as in [L2], S^*_1 is irreducible, the branch locus of S^*_1 over S is contained in $S_1 \cap \Delta$ and hence consists of at most two points and $k(S^*_1)$ is a galois extension of $k(S_1)$ with galois group isomorphic to S_n. Since $k(S_1)/k$ is simply transcendental, we are through by invoking Lemma A3 of Section 8.

PROPOSITION 6. *Let L be a finite algebraic extension of K with* $[L:K]$

$= m > 1$. *Then* (I) *there is at least one valuation of* K/k *which is ramified in* L. (II) *If there is only one valuation of* K *which is ramified in* L, *then it must be nontamely ramified.* (III) *If* L/K *is tamely ramified and if there are only two valuations of* K/k *which are tamely ramified in* L, *then* L/K *is cyclic and* $m \not\equiv 0 \pmod p$ *in case* $p \neq 0$. (IV) *Given two valuations* v_1 *and* v_2 *of* K/k *and an integer* n *such that* $n \not\equiv 0 \pmod p$ *in case* $p \neq 0$, *there exists a unique (up to a* K*-isomorphism) tamely ramified cyclic extension* L *of* K *of degree* n *such that* v_1, v_2 *are the only valuations of* K/k *ramified in* L.

Proof. Let $g =$ genus of L/k and $\lambda =$ degree of the difference of L over K. By [Corollary 2, p. 106 of C], $2g = \lambda - 2m + 2$. Since $g \geqq 0$ and $m > 1$ we have $\lambda \geqq 2m - 2 \geqq m > 0$ which proves (I).

Now assume that L/K is tamely ramified, let v be a valuation of K and let $w_1, w_2, \cdots, w_t$ be the valuations of L lying above v; then the contribution $\lambda(v)$ of v to λ is given by $\lambda(v) = \sum_{i=1}^{t} [d(w_i : v) - 1] = m - t \leqq m - 1$. Hence if q valuations of K are ramified in L then $\lambda \leqq q(m-1)$; since $\lambda \geqq 2m - 2 = 2(m-1)$ we must have $q \geqq 2$. Now assume that $q = 2$, let v_1 and v_2 be the valuations of K which are ramified in L, let L^* be a least galois extension of K containing L and let t_1 and t_2 be the number of valuations of L^* lying above v_1 and v_2 respectively, let λ^* be the degree of the different of L^*/K and let $m^* = [L^* : K]$. Then $2m^* - (t^*_1 + t^*_2) = (m^* - t^*_1) + (m^* - t^*_2) = \lambda^* \geqq 2m^* - 2$, hence $t^*_1 = t^*_2 = 1$; therefore the galois group G of L^*/K equals the splitting group S over v_1 of the L^*-extension of v_1. Since v_1 is tamely ramified in L, it follows by Proposition 7 of Section 5 that v_1 is tamely ramified in L^* and hence S is cyclic and $m^* \not\equiv 0 \pmod p$. Therefore $L = L^*$. This proves (II) and (III).

A proof of (IV) and a reproof of (II) and (III), all this using only (I), can at once be obtained by the method and results of Section 6.

Remark 5. In the classical case when k is the field of complex numbers, parts (I) and (II) correspond to Proposition T1 and T2 (Section 7), respectively, and parts (III) and (IV) correspond to Proposition T3.II (Section 7).

4. Algebraic fundamental groups and universality. For the sake of definiteness in this section we shall assume that the field of definition of all varieties concerned is a fixed algebraically closed field k of characteristic p.

4.1. *Definitions.* Let F be a *family* of finite groups, given another family F_1 of finite groups we shall regard F and F_1 to be the same families, i.e., $F = F_1$, if f is in F implies there exists f_1 in F_1 isomorphic to f and conversely. Let G be a group (finite or infinite) and let p be a prime number. We make the following definitions:

$(F)^p =$ the family of members of F whose order is prime to p.

$F_s =$ the family of subgroups of members of F.

$F_h =$ the family of homomorphic images of members of F.

$G_h =$ the family of finite homomorphic images of G.

Observe that $F_{shs} = F_{shh} = F_{sh}$ (proof is trivial). Let ϕ be a property of finite groups. F is said to be ϕ if each member of F is ϕ, F is said to be *not* ϕ if at least one member of F is not ϕ, F is said to be *non* ϕ if each member of F is non ϕ. Thus F is abelian means each member of F is abelian, F is not abelian means at least one member of F is nonabelian, and F is nonabelian means each member of F is nonabelian. F is said to be *complete* if F equals the family of *all* finite groups. Observe that many important properties are shared by F, F_s and F_{sh} simultaneously; for instance this is so for the following properties: (1) being abelian, (2) being solvable, (3) being a p-group for a fixed p, (4) being a p-group for various p; i.e., F is abelian if and only if F_s is abelian, if and only if F_{sh} is abelian, and so on. Also note that if $\{F_a\}_{a \in A}$ is a collection of families of finite groups and if the unions are taken over the indexing set A, then $(UF_a)_s = (UF_{as})$, $(UF_{ah}) = (UF_a)_h$ and the same for intersections. For a finite group G we shall denote by $p(G)$ the (normal) subgroup of G generated by all the p-sylow subgroups of G; recall [see A3] that G is called a *quasi* p-group if $G = p(G)$; the family of all quasi p-groups will be denoted by $Q(p)$.

Let V be a normal variety and D a proper subvariety of V. If K^* is a finite algebraic extension of $k(V)$ and V^* is a K^*-normalization of V then the branch locus on V for the transformation between V and V^* will be denoted by $\Delta(V^*/V)$ or by $\Delta(K^*/V)$. Now we define:

(1) $\Omega(V - D) =$ the family of finite algebraic extensions L of $k(V)$ for which $\Delta(L/V) \subset D$.

(2) $\Omega_g(V - D) =$ the family of members L of $\Omega(V - D)$ such that $L/k(V)$ is galois.

(3) $\Omega'_g(V - D) =$ the family of members L of $\Omega_g(V - D)$ such that L/V is tamely ramified.

(4) $\Omega^*_g(V-D)=$ the family of members L of $\Omega_g(V-D)$ such that $[L:k(V)]\not\equiv 0 \pmod{p}$ in case $p\neq 0$ (and no restriction if $p=0$).

(5) $\pi_A(V-D)$, $\pi'_A(V-D)$, $\pi^*_A(V-D)$
$=$ the family of galois groups of $L/k(V)$ for members L of $\Omega_g(V-D)$, $\Omega'_g(V-D)$, $\Omega^*_g(V-D)$, respectively.

(6) $\pi_B(V-D)$, $\pi'_B(V-D)$, $\pi^*_B(V-D)$
$=[\pi_A(V-D)]_s$, $[\pi'_A(V-D)]_s$, $[\pi^*_A(V-D)]$, respectively.

(7) $\pi_C(V-D)$, $\pi'_C(V-D)$, $\pi^*_C(V-D)$
$=[\pi_B(V-D)]_h$, $[\pi'_B(V-D)]_h$, $[\pi^*_B(V-D)]_h$, respectively.

Now let P be a point on V. Then we define:

(L1) $\Omega(V-D,P)=$ the family of finite algebraic extension L of $k(V)$ for which the components of $\Delta(L/V)$ passing through P are contained in D.

(L2) $\Omega_g(V-D,P)=$ the family of members L of $\Omega(V-D,P)$ such that $L/k(V)$ is galois.

(L3) $\Omega'_g(V-D,P)=$ the family of members L of $\Omega_g(V-D,P)$ such that P is tamely ramified in L.

(L4) $\Omega^*_g(V-D,P)=$ the family of members L of $\Omega_g(V-D,P)$ such that for a point Q corresponding to P on the L-normalization of V we have $d(Q:P)\not\equiv 0 \pmod{p}$ in case $p\neq 0$ (and no restriction if $p=0$).

(L5) $\pi_A((V-D,P)$, $\pi'_A(V-D,P)$, $\pi^*_A(V-D)$
$=$ the family of splitting groups over $k(V)$ of points corresponding to P on the L-normalization of V for members L of $\Omega_g(V-D,P)$, $\Omega'_g(V-D,P)$, $\Omega^*_g(V-D,P)$, respectively.

(L6) and (L7): Similar to (6) and (7), respectively.

(8) We shall say that $V-D$ is respectively (I) universal, (II) strongly universal, (III) modelwise universal, and (IV) modelwise strongly universal, or, respectively, that (I′) D is a universal branch locus for V,

(II') · · ·, (III') · · ·, (IV') if, respectively, the following conditions hold: (CI) given a finite algebraic extension K^* of $k(V)$ there exists L in $\Omega(V-D)$ such that L is k-isomorphic to K^*; (CII) given a finite algebraic extension K^*_1 of $k(V)$ and a finite algebraic extension K^*_2 of K^*, there exists L_2 in $\Omega(V-D)$ and L_1 with $K\subset L_1\subset L_2$ such that there is a k-isomorphism of L_2 onto K^*_2 which maps L_1 onto K^*_1; (CIII) given a finite alegbraic extension K^* of $k(V)$ there exists L in $\Omega(V-D)$ such that the normalizations of V in L and K^* can be mapped onto each other biregularly; (CIV) · · · such that the normalizations of V in L_2 and K^*_2 can be mapped onto each other by a biregular map which induces a biregular map between the normalizations of V into L_1 and K^*_1. It is clear that (CII) is equivalent to: given a finite sequence of finite algebraic extension $k(V)\subset K^*_1\subset K^*_2\subset\cdots\subset K^*_n$, there exist $k(V)\subset L_1\subset L_2\subset\cdots\subset L_n$ in $\Omega(V-D)$ and a k-isomorphism of L_n onto K^*_n which maps L_i onto K^*_i for $i=1,2,\cdots,n$; and similarly, for (CIV). Furthermore, D will be said to be a *minimal universal* (respectively strongly universal, modelwise universal, modelwise strongly universal) branch locus for V if D is a universal (respectively s. u., m. u., m. s. u.) branch locus for V and if no proper subvariety of D is such.

Observe that if V is one-dimensional, then things depend only on $k(V)$ and the set of valuations corresponding to the points of D; hence we may replace the models by their function fields.

Having made all these definitions, we now turn to results, conjectures and comments.

4.2. *Fundamental groups.* If k is the field of complex numbers, and if the (corresponding Riemann type) existence theorem for $V-D$ is available, then $(\pi_1(V-D))_h=\pi_A(V-D)$ where π_1 is the topological fundamental group. Although π_1 besides giving $(\pi_1)_h$ also gives the manner in which these groups are intertwined together, nevertheless $(\pi_1)_h$ and hence π_A is a good algebraic approximation to π_1 [of course, eventually one may have to consider the galois group over $k(V)$ of the compositum of all the galois group over $k(V)$ of the compositum of all the members of $\Omega(V-D)$ which one expects to be the Krull-completion of $\pi_1(V-D)$]. For instance, π_1 is free with n generators implies $(\pi_1)_h$ consists of all finite groups with n generators; π_1 is abelian implies $(\pi_1)_h$ is abelian and so on. Since, as has been indicated, important properties are carried simultaneously by π_A, π_B, π_C, it is quite worthwhile, lacking a knoweldge of π_A itself, to study π_B or π_C. Exactly similar comments are valid for the local situation $V-D,P$.

Concerning ramification theory in the abstract case, we offer the following two general conjectures. For $p\neq 0$ let S_p be a situation either of type $V-D$ or of type $V-D,P$; and let S_0 be the *corresponding situation in characteristic zero* (i.e., in the classical case). Then, roughly speaking:

$$(\text{ramification theory for } S_p) = (\text{ramification theory for } S_0) + Q(P);$$

or better:

$$(\text{ramification theory for } S_p)/Q(P) = (\text{ramification theory for } S_0);$$

and now more precisely:

CONJECTURE 1. $\pi_A(S_p)$ *= the family of all finite groups* G *such that* $p(G)\in Q(p)$ *and* $G/p(G)\in\pi_A(S_0)^p$.

CONJECTURE 2 (*Supplement to Conjecture* 1).

$$(\pi_A(S_0))^p=\pi^*{}_A(S_p)\subset\pi'{}_A(S_p)\subset\pi_A(S_0)$$

and the last inclusion is a near equality.

Conjecture 1 consists of three steps: (1) to algebraize π_1 in the classical case, see Remark 7; (2) to show that *for a situation* S_p *for which there exist nontrivial coverings, then all members of* $Q(P)$ *are realizable*; and (3) to do the extension problem for (1) and (2). Let us call step (2), *Conjecture* 1.1; and the much weaker form of 1.1, where we replace $Q(p)$ *by the family of all p-groups,* let it be called *Conjecture* 1.2.

These conjectures on π_A reflect in π_B or π_C in a diluted form. To illustrate the meaning of "corresponding situation" by examples: (1) S_p = line minus n points, S_0 = same; (2) S_p = curve of genus g, S_0 = same; (3) S_p = projective plane minus a curve with ordinary double points and components of orders $n_1,n_2,\cdots,n_t$, S_0 = same; (4) S_p = projective n space minus m hyperplanes in general position, S_0 = same; now some local examples: (5) S_p = (V = projective plane, D = a curve, P = a point at which D has a certain type of singularity), S_0 = $(\cdot\cdot\cdot,\cdot\cdot\cdot,\cdot\cdot\cdot D$ has the *corresponding* type of singularity). Now for certain situations S_p there may not exist a corresponding S_0; for such S_p the conjectures of course would not apply, for instance in the last example for S_p, P may be a point of D at which there is no Puiseux expansion! For the local theory, a bit of evidence for the conjectures is given in our previous papers [A1] and [A3]; observe that for the local theory, in case of dimension one, $Q(p)$ has to be replaced by the family of all p-groups [see K]. For the global theory, when V is one-dimensional, the following evidence results from this paper:

Let C be a nonsingular algebraic curve over an algegraically closed ground field k of characteristic p, and let D_n be a set of n (distinct) points of C.

Result 1. In the classical case by Proposition T3, there are only a finite number of (non $k(C)$-isomorphic) members of $\Omega(C-D_n)=\Omega'(C-D_n)$ of a given degree over $k(C)$; by Theorem 5 (Section 6) this is so for any p with $\Omega'(C-D_n)$.

Result 2. (Trivial) $\Omega(C-D_0)$ and $\Omega'(C-D_1)$ are empty (except for C) and $\Omega'(C-D_2)$ consists of all cyclic extensions (of degree prime to p if $p\neq 0$); Proposition 6 and Remark 5 (Section 3).

Now we assume that $C=$ a projective line L (or any rational curve).

Result 3. Let $n\geqq 3$. By Proposition T4 (Section 7) in the classical case $\pi_B(L-D_n)$ is complete. To support the part of Conjecture 2 which says that $\pi'_A(S_p)$ is nearly equal to $\pi_A(S_0)$, we might expect that for arbitrary p not only $\pi_B(L-D_n)$, but even $\pi'_B(L-D_n)$ is complete. *For* $p\neq 2$ *it follows from Proposition* 3 *that* $\pi'_B(L-D_n)$ *is complete, while for* $p=2$, *Proposition* 5 *gives the weaker result that* $\pi_B(L-D_n)$ *is complete* [in fact Proposition 5 yields the stronger conclusion that $\pi_B(L-D_2)$ is complete]. Furthermore by Proposition T3 (Section 7) in the classical case $\pi_A(L-D_n)$ contains all the finite groups generated by two generators and hence in particular for any integer m the symmetric group on m letters: *in the abstract case, we have proved in Proposition* 3 *that* $\pi'_A(L-D_n)$ *contains the symmetric group on* m *letters if* $p=0$ *and if* $p\neq 0$ *then provided either* $m, m-1\not\equiv 0 \pmod{p}$ *or* m *is odd and* $m, m-2, 2\not\equiv 0$ $(\operatorname{mod} p)$.

Result 4. Assume $p\neq 0$. Now Proposition 6 tells us that $\pi_A(L-D_1)\subset Q(p)$ while, in view of Theorem 1, Conjecture 1.1 implies that $\pi_C(L-D_1)=Q(p)\supset$ (family of all simple groups whose orders are divisible by p) $\supset$ the alternating groups on m letters for all $m\geqq p$); this would tend to imply that $\pi_C(L-D_1)$ is complete. Now it does follow from Theorem 2 and Propositions 3 and 5 that *indeed* $\pi_C(L-D_1)$ *is complete.*

Remark 6. It follows from Result 4 that $\pi_A(L-D_1)$ contains (plenty of them) unsolvable groups, i.e., the affine line $L-D_1$ has unsolvable unramified coverings and hence in particular nonabelian ones. This is surprising since the affine in line is a commutative group variety. Note that in [L1] Lang had obtained nonabelian coverings only for noncommutative group varieties. It would be interesting to characterize the possible galois groups of unramified coverings of commutative group varieties in general.

Remark 7. The main problem in algebraizing π_1 is to prove Theorem T (Section 7) algebraically, i. e., to prove Theorem T is the abstract case (for any charatceristic) restricting attention to tamely ramified extensions only (in which case we conjecture the theorem to be true). However, even part (III) of Theorem T is false for nontamely ramified extensions, thus: By Remark 6 there exists a galois covering of L with unsolvable galois group G and ramified only in D_1 while the splitting group S of any point above D_1 is solvable [K] and hence S cannot possibly generate G; really! it is unnecessary to be so round-about, for part (III) of Theorem T, if true in general, would imply that if there is only one branch point D_1 on L then D_1 cannot split (by itself); and in Theorem 1 this has been proved false for nontamely ramified extensions. Thus (alas!) for nontamely ramified extensions not only with L with one puncture is nonsimply connected (which has been well known), but the monodromy group is not even generated by the loops around the branch points (Section 7).

4. 3. *Universality.* We may state Theorem 4 as

Result 5. If $p \neq 0$ then for a projective line L over k, any one point of L is a minimal universal as well as minimal strongly universal branch locus for L.

We note that universality is a typical nonzero characteristic concept meaning thereby for characteristic zero one excepts that a universal branch locus could never exist, for instance if L is the projective line over k and D_n a set of n points of L and $p = 0$, then (by Theorem 5 of Section 6) the number of non $k(C)$-isomorphic members of $\Omega(L - D_n)$ is countable (i. e., of cardinality less than or equal to that of the set of integers) and *a fortiori* the number of non k-isomorphic members of $\Omega(L - D_n)$ is countable; if now we assume that k is of uncountable cardinality (for instance, $k =$ complex numbers) then there are uncountably many non k-isomorphic extensions of $k(L)$ as follows for instance, since the moduli varieties are positive dimensional varieties over k; hence L has no universal branch locus (this cardinality argument is due to Serre; one should find a proof without the cardinality assumption). However, for a field k of nonzero characteristic, we have

CONJECTURE 3. *Every curve C over k has universal branch loci.*

After proving this conjecture, one should find the comomn properties shared by all the minimal universal branch loci of C; that should yield new (birational) invariants for C. Given a curve over a field of characteristic zero, reducing it modulo various primes would then yield invariants of the original curve for each of these primes. It is clear that if in the definition of universality, we replace overfields by subfields, then there results another concept which we may call *antiuniversality*; it would be interesting to investigate this as well.

5. Least galois extensions. Let K be a one-dimensional algebraic function field over an algebraically closed ground field k of characteristic p. Let L be a finite separable algebraic extension of K and let L^* be a least galois extension of K containing L and let $\Lambda(L/K)$ and $\Lambda(L^*/K)$ denote respectively the differents of L and L^* over K. It is convenient to have a formula expressing $\Lambda(L^*/K)$ in terms of $\Lambda(L/K)$ (it would give the genus of L^* in terms of the genus of K). This can, for instance, be used in studying the following question: What kind of function fields L^* (and what kind of galois groups) can be obtained as the least galois extension of a simple transcendental extension of k containing another simple transcendental extension of k; in other words, given L^*/k under what condition can we find x and t in L^* such that $k(t) \subset k(x)$ and L^* is a least galois extension of $k(t)$ containing $k(x)$? The study of such L^* is facilitated due to the fact that it is gotten by a covering of a line by a line. In this section, we obtain such a formula provided L is tamely ramified over K. Let $v_1, v_2, \cdots, v_t$ be the valuations of K/k which are ramified (tamely) in L; then these are exactly the valuations of K which are ramified in L^* (Proposition 1 of A1). Let $v_{i1}, v_{i2}, \cdots, v_{ia_i}$ be the valuations of L^* lying above v_i and let $w_{i1}, w_{i2}, \cdots, w_{ib_i}$ be the valuations of L^* lying above v_i. Let $d(v_{ij}:v_i) = e_{ij}$ and $d(w_{ij}:v_i) = f_i$ [since L^*/K is galois $d(w_{ij}:v_i)$ does not depend on j]. Then the formula is $f_i = [e_{i1}, e_{i2}, \cdots, e_{ia_i}]$ where the square brackets denote the least common multiple, in other words,

$$\text{if } \Lambda(L/K) = \prod_{i=1}^{t} \prod_{j=1}^{a_i} v_{ij}{}^{e_{ij}-1}, \text{ then } \Lambda(L^*/K) = \prod_{i=1}^{t} \prod_{j=1}^{b_i} w_{ij}{}^{[e_{i1}, \cdots, e_{ia_i}]-1}$$

where in each equation the first product sign is taken over all valuations v_i of K/k and the second product sign is taken over all the valuations respectively of L and L^* lying above v_i (for unramified v_i the corresponding exponents of v_{ij} and w_{ij} are zero). This formula is motivated by Proposition T5 (Section 7) for the classsical case where k is the field of complex numbers and K/k is simple transcendental. Now to the proof. We start with a remark on compositums of fields.

Let K be a field and let $K_1, K_2, \cdots, K_t$ be finite algebraic extensions of K. Recall that an extension K^* of K is called a K-compositum of $K_1, \cdots, K_t$ if K^* contains subfields $K'_1, \cdots, K'_t$ containing K such that K^* is generated over K by $K'_1, \cdots, K'_t$ and K'_i is K-isomorphic to K_i for $i = 1, \cdots, t$. To see that K^* exists it is enough to take an algebraic closure Ω of K, to take for $i = 1, \cdots, t$ subfields K'_i of Ω containing K and K-isomorphic to K_i and to let K^* be the compositum of $K'_1, \cdots, K'_t$ *in* Ω.

Now let $L_1, L_2, \cdots, L_t$ be least normal extension of K containing $K_1, K_2, \cdots, K_t$ respectively. Let L^* be a K-compositum of $L_1, \cdots, L_t$. Then L^*/K is normal (obvious) and is uniquely determined up to isomorphism by the extensions $L_1/K, \cdots, L_t/K$, i.e., if L^{**} is any other K-compositum of $L_1, \cdots, L_t$, then there exists a K-isomorphism τ from L^* onto L^{**} such that if f_i and g_i are the given isomorphisms of L_i onto subfields L'_i and L''_i of L^* and L^{**} respectively, then $f_i\tau = g_i$. For fix a polynomial $A_i(X)$ in $K[X]$ such that L_i is a root field of $A_i(X)$ over K, our assertion then follows from the fact that L'_i is *the* root field of $A_i(X)$ over K *in* L^* [hence $f_i(L_i)$ as a subfield of L^* depends only on L_i and not on f_i] and hence L^* is a root field of $A(X) = A_1(X)A_2(X) \cdots A_t(X)$ over K. The same argument shows that L^* can also be defined as a least normal extension of a K-compositum of $K_1, \cdots, K_t$. We shall call L^* *a least normal K-compositum of* $K_1, \cdots, K_t$.

LEMMA 1. *Let K/k be an r-dimensional algebraic function field, let L be a finite separable algebraic tension of K and let L^* be a least galois extension of K containing L. Let R be the quotient ring of a point on a normal projective model of K/k. Let $S_1, \cdots, S_t$ be the local rings in L lying above R and let S^* be any local ring in L^* lying above R. Let $\bar{R}$ be a completion of R and let $\bar{K}$ be a quotient field of $\bar{R}$ containing K. Let $\bar{S}_i$ be a completion of S_i canonically containing $\bar{R}$ and let $\bar{L}_i$ be a quotient field of $\bar{S}_i$ containing $\bar{K}$ and L. Let $\bar{S}^*$ be a completion of S^* canonically containing $\bar{R}$ and let $\bar{L}^*$ be a quotient field of $\bar{S}^*$ containing $\bar{K}$ and L^*. Then* (I) *$\bar{L}^*$ is a least normal $\bar{K}$-composition of $\bar{L}_1, \bar{L}_2, \cdots, \bar{L}_t$. Let $f(X)$ be the minimal monic polynomial of a primitive element of L/K. Let x be a root of $f(X)$ in L, then* (III) *x as an element of $\bar{L}_i$ is a primitive element of $\bar{L}_i/L$, so that* (IV) *$\bar{L}_i$ is the compositum of L and $\bar{K}$ in $\bar{L}_i$, and if we let $f_i(X)$ be the minimal monic polynomial of x over $\bar{K}$, then* (V)

$f(X) = f_1(X) f_2(X) \cdots f_t(X)$ is the factorization of $f(X)$ into pairwise coprime irreducible factors in $\bar{K}[X]$.

Proof. (III) and (V) are proved in Proposition 1 of [A2] in the case where x is integral over R, however this implies that $\bar{L}_i$ is the compositum of L and $\bar{K}$ *in* $\bar{L}_i$ and hence any primitive element x of L/K is a primitive element of $\bar{L}_i/\bar{K}$ which proves (III) and (IV); again since for a suitable nonzero element c in R, cx is integral over R, Proposition 1 of [A2] gives (V) for cx which in turn implies (V) for x. Now (IV) applied to S^* tells us that $\bar{L}^*$ is the compositum of L^* and $\bar{K}$ in $\bar{L}^*$ and since L^*/L is given by the roots of $f(X)$, we obtain (II). Finally (I) follows from (II) and (V).

LEMMA 2. *Let $E = k((x))$ be the power series field in one variable over an algebraically closed field k of characteristic p and let E^* be a finite algebraic extension of E with $[E^*:E] = n$ such that $n \not\equiv 0 \pmod{p}$ if $p \neq 0$. Then $E^* = E(x^{1/n})$.*

Proof. This proof is well known.

PROPOSITION 7. *In Lemma 1, assume that k is algebraically closed and $r = 1$ and R is tamely ramified in L and let $d(S_i:R) = n_i$. Then $d(S^*:R) = [n_1, n_2, \cdots, n_t]$, (and hence R is tamely ramified in L^*).*

Proof. R is normal, $r = 1$ and k is algebraically closed implies that $\bar{K} = k((x))$ where x is a regular parameter in R. By Lemma 2, $\bar{L}_i = \bar{K}(x^{1/n_i})$ and hence by Lemma 1. I, $\bar{L}^* = \bar{K}(x^{1/[n_1, \cdots, n_t]})$ so that $d(S^*:R) = [\bar{L}^*:\bar{K}]$ $[n_1, n_2, \cdots, n_t]$.

Remark 8. Is there a corresponding formula if we omit the assumption of tame ramification?

6. Finiteness of the number of coverings with assigned branch points.

In their recent paper, Lang and Serre have proved [Theorem 4 of LS] that if K is a one-dimensional algebraic function field over an algebraically closed ground field k of characteristic p, then for any given integer n the number of non K-isomorphic unramified extensions of K of degree n is finite. Here we extend this result to extensions with assigned branch points (this is done by using a globalized form of a trick which we had used in [A1] for focal purposes), namely

THEOREM 5. *Let V be a given finite set of valuations of K/k and let n be a positive integer. Then the number of non K-isomorphic tamely* *ramified extensions K^* of K of degree n such that $\Delta(K^*/K)$ is contained in V is finite.*

We first prove two propositions.

PROPOSITION 8. *Let K^* be a finite separable algebraic extension of a one-dimensional algebraic function field K over an algebraically closed ground field k of characteristic p. For $y \in K$, $y \notin k$, let K^*_1 be a root field of $X^g - y$ over K^* where $g \not\equiv 0 \pmod{p}$ if $p \neq 0$ and let K_1 be the root field of $X^g - y$ over K in K^*_1. Let v^*_1 be a valuation of K^*_1/k and let v^*, v_1, v be the restrictions of v^*_1 to K^*, K_1, K respectively. Let $h = v(y)$, $n = d(v^*:v)$, $q = (g,h)$, $g_1 = g/q$, $q^* = (g_1, n)$, $N^* = g_1/q^*$ and $N = n/q^*$ [parenthesis denotes the greatest common divisor]. Then* (I) *$d(v^*_1:v_1) = N$ and $d(v^*_1:v^*) = N^*$.* (II) *If $h = v(y) = 1$ and $g \equiv 0 \pmod{n}$ then $N = d(v^*_1:v_1) = 1$.* (III) *If $d(v^*:v) = 1$ then $d(v^*_1:v_1) = 1$; this remains true if K^*_1 is replaced by any finite separable algebraic extension of K^* and K_1 is replaced by a subfield of K^*_1 containing K such that K^*_1 is the compositum of K_1 and K^*.*

Proof. Fix x in K with $v(x) = 1$. Then $y = x^h\delta$ where $\delta \in K$ with $v(\delta) = 0$. Let z be a root of $X^g - y$ in K^*_1. Let $E = k((x))$ and let E^*_1 be a v^*_1-completion of K^*_1 so that E becomes the corresponding v-completion of K, let E^* and E_1 be the sufields of E^*_1 which are the corresponding completions of K^* and K_1 respectively, then [Proposition 1 of A2] $E^*_1 = E^*(z)$ and $E_1 = E(z)$, also $[E^*_1:E_1] = d(v^*_1:v_1)$, $[E^*_1:E^*] = d(v^*_1:v^*)$ and $[E^*:E] = d(v^*:v) = n$. Since $g \not\equiv 0 \pmod{p}$ if $p \neq 0$ and δ is a unit in $k[[x]]$, there exists a unit e in $k[[x]]$ such that $e^g = \delta^{-1}$ and we have $(ze)^g = z^g e^g = x^h \delta e^g = x^h$. Hence, by replacing z by ze we may assume that $y = x^h$. Now it follows from Lemma A5 (Section 8) that $[E^*_1:E_1] = N$ and $[E^*_1:E^*] = N^*$ which proves (I), while (II) follows at once from (I). In the present case (III) follows from (I) while in the general case it can be proved directly as follows: Let E^*_1 be a v^*_1-completion of K^*_1 and let E_1, E^*, E be the corresponding completions of K_1, K^*, K respectively. Let z be a primitive element of K^*/K so that z is also a primitive element of K^*_1/K_1 and hence [Proposition 1 of A2] $E^* = E(z)$ and $E^*_1 = E_1(z)$; now $d(v^*:v) = 1$ means $[E^*:E] = 1$, i.e., $z \in E^*$ and hence $z \in E_1$, so that $d(v^*_1:v_1) = [E^*_1:E_1] = 1$.

PROPOSITION 9. *Let K^* be a finite separable algebraic extension of a one-dimensional algebraic function field K over an algebraically closed ground field k of characteristic p. Let L^* be a finite separable algebraic extension* *of* K^* *and let* L *be a subfield of* L^* *containing* K *such that* L^* *is the compositum of* L *and* K^*. *Let* w^* *be a valuation of* L^*/k *and let* w, v^*, v *be the restrictions of* w^* *to* L, K^*, K *respectively. Let* $n = d(v^*:v)$. *Assume that there exists* $z \in L$ *and a positive integer* g *divisible by* n *with* $g \not\equiv 0 \pmod{p}$ *if* $p \neq 0$ *such that* $z^g \in K$ *and* $v(z^g) = 1$. *Then* $d(w^*:w) = 1$.

Proof. Let $K_1 = K(z)$, $K^*_1 = K^*(z)$. Apply Proposition 8. II to K^*_1, K_1, K^*, K and then apply Proposition 8. III to L^*, L, K^*_1, K_1.

Proof of Theorem 5. We may restrict our attention to the extensions of K in a fixed algebraic closure Ω of K. It is enough to prove that there exists a finite number of finite separable algebraic extensions $L_1, L_2, \cdots, L_q$ of K such that if K^* is a tamely ramified algebraic extension of K of degree n with $\Delta(K^*/K) \subset V$ then for some L_T the compositum L^*_T of L_T and K^* is unramified over L_T. For then each such K^* will be contained in an unramified extension L^*_T of some L_T with $[L^*_T : L_T] \leqq n$. By the Serre-Lang theorem, the number of these L^*_T is finite for each T and hence the number of fields between L^*_T and K for the various L^*_T for the various L_T $(T = 1, \cdots, q)$ is finite; hence *a fortiori* the number of extensions K^*/K of the said type is also finite.

Proposition 9 gives us various ways of constructing extensions $L_1, \cdots, L_q$ with the required properties. Let $v_1, v_2, \cdots, v_t$ be the valuations in V; fix y_i in K with $v_i(y_i) = 1$. Let $M_T = \{(M_{Ti1}, M_{Ti2}, \cdots, M_{TiT_i})\ M_{Tij} > 0, \not\equiv 0 \pmod{p}$ if $p \neq 0$; $M_{Ti1} + M_{Ti2} + \cdots + M_{TiT_i} = n$ for $i = 1, 2, \cdots, t\}$ with $T = 1, 2, \cdots, q$ be the various simultaneous (for $i = 1, 2, \cdots, t$; i. e., t at a time) partitions of n into positive integers which are prime to p if $p \neq 0$. For $T = 1, 2, \cdots, q$ let

$$f_T(X) = \prod_{i=1}^{t} \prod_{j=1}^{T_i} (X^{M_{Tij}} - y_i),$$

and let L_T be the root field of $f_T(X)$ over K. Then given K^* (of the said type) there is a (unique) T such that for $i = 1, 2, \cdots, t$ the degrees over v_i of the various extensions of v_i to K^* are $M_{Ti1}, M_{Ti2}, \cdots, M_{TiT_i}$; and hence by Proposition 9, the compositum of L_T and K^* is unramified over L_T.

Also we can, in various ways, manage that it will be enough to take one single L. Firstly, we can take for L the root field over K of $f_1(X) f_2(X) \cdots f_q(X)$. Secondly, letting N to be the product of all positive integers which are less than or equal to n and which are prime to p if $p \neq 0$, we can take for L the root field over K of $(X^N - y_1)(X^N - y_2) \cdots (X^N - y_t)$. Thirdly, by the theorem of independence of valuations there exists $y \in K$

such that $v_i(y) = 1$ for $i = 1, 2, \cdots, t$; and we may take for L the root field of $X^N - y$ over K.

That the condition of tame ramification is essential is well known. For instance, let $K = k(x)$ be simple transcendental with k algebraically closed of characteristic $p \neq 0$ and let K^*_m be a root field over K of $f_m(X) = X^p - X - x^m$ where m is any positive integer prime to p. Then K^*_m/K is cyclic of degree p. Since $f'_m(X) = -1$, $v: x = \infty$ is the only valuation of K/k which is possibly ramified in K^*_m. Let z be a root of $f_m(X)$. Then $K^*_m = k(z)(x)$ and $g_m(X) = X^m + z - z^p$ is the minimal monic polynomial of x over $k(z)$. Let w_i be the valuation of $k(z)/k$ given by $z = i$ for $i = 1, 2, \cdots, p$ and let w_∞ be the valuation of $k(z)/k$ given by $z = \infty$. Then $Dg_m(X) = (z - z^p)^{m-1}$ so that $w_1, \cdots, w_p, w_\infty$ are the only valuations of $k(z)/k$ which are possibly ramified in K^*_m. Also $w_i(x^m) = 1$ for $i = 1, \cdots, p$ and $w_\infty(x^m) = -1$ imply that there are unique valuations $w^*_1, \cdots, w^*_p, w^*_\infty$ of K^*_m lying above $w_1, \cdots, w_p, w_\infty$ respectively and $d(w^*_i : w_i) = m \not\equiv 0 \pmod{p}$ for $i = 1, 2, \cdots, p, \infty$. Therefore the genus g_m of K^*_m/k is given by: $g_m = (\frac{1}{2})(p+1)(m-1) - m + 1 = (\frac{1}{2})(p-1)(m-1)$. Hence for the various values of m the extensions K^*_m are of distinct genera so that they are non k-isomorphic and hence *a fortiori* non K-isomorphic.

Remark 9. Presumably one can at once generalize Theorem 5 to higher dimensional varieties by taking a generic plane section and applying Theorem 5.

7. Some topological considerations in the classical case.

In this section, we shall not try to be completely precise since logically the contents of this section do not belong in this paper and are used only for descriptive, motivating, and comparative purposes. For well-known properties of topological coverings to be used, we refer for instance to Part I of [S2].

Let K be a pure transcendental extension of the field k of complex numbers, and let L be a finite algebraic extension of K with $[L:K] = n > 1$. Let T be the Riemann surface of L/k, i.e., the set of all valuations of L/k topologized in the classical fashion and let S be the Riemann surface of K/k; then S is the Riemann sphere and T is a ramified covering of S, let f be the projection of T onto S, let D be the set of points of S which are ramified in L and let E be the set of points of T lying above the points of D, then $T - E$ is an unramified covering of $S - D$; we may think of S as the euclidean plane R together with a point P_∞ at infinity. Since S as well as R are simply connected, D must contain more than one point and we may state

PROPOSITION T1. *There are no unramified proper extensions of K/k.*

PROPOSITION T2. *There are no proper extensions of K/k which are ramified only at one valuation of K/k.*

Let γ be an arc in $S - D$ from a point X_0 to a point X_1, let Y_0 be any point in $f^{-1}(X_0)$, then there exits a unique arc δ in $T - E$ starting at Y_0 and lying over γ, let Y_1 be the point of δ lying avove X_1; thus γ gives rise to a mapping of $f^{-1}(X_0)$ into $f^{-1}(X_1)$ which we shall denote by $h(\gamma)$; observe that h is multiplicative; now $h(\gamma)$ does not change if we vary γ by a homotopy (stationary at X_0 and X_1) and hence we obtain a mapping from the homotopy classes of arcs in $S - D$ into the class of mappings of the fibres of their starting points into the fibres of their end points; this mapping we shall also denote by h; the restriction of h to the loops at a point X_0 then gives the homomorphism of $\pi_1(S - D, X_0)$ into the group of permutations of $f^{-1}(X_0)$ and this will again be denoted by h; which particular meaning of h is to be taken will always be obvious from the context. For a point X_0 in $S - D$ we shall denote $h(\pi_1(S - D, X_0)$ by $H(X_0)$. Let P be a given point in D, we may assume that P_∞ is any point of D other than P; let $Q_1, Q_2, \cdots, Q_t$ be the points in $f^{-1}(P)$ and let $d(Q_i : P) = r_i$. Let A be a small closed circular neighborhood with center P (not containing any other points of D); then the use of uniformizing parameters at once shows that the connected components of $f^{-1}(A)$ are neighborhoods $B_1, B_2, \cdots, B_t$ of $Q_1, Q_2, \cdots, Q_t$ respectively and $B_i - Q_i$ is an r_i-fold cyclic covering of $A - P$. Let a be the positively oriented (with respect to a fixed orientation of S) boundary of A. Let M be a point on a and let $N_{i1}, N_{i2}, \cdots, N_{ir_i}$ be the points in B_i lying above M. Now a is a deformation retract of $A - P$ stationary at M and hence a generates $\pi_1(A - P, M)$. Therefore the action of a on $N_{i1}, N_{i2}, \cdots, N_{ir_i}$ is to permute them cyclically, i.e., if for each fixed i we arrange the N_{ij} suitably, then the action of a is given by the r_i-cycle $(N_{i1}, N_{i2}, \cdots, N_{ir_i})$. Hence the action of a on $f^{-1}(M)$, i.e., $h(a)$, is the permutation on the $r_1 - r_2 + \cdots + r_t = n$ points N_{ij} which is the product of the t disjoint cycles $(N_{i1}, N_{i2}, \cdots, N_{ir_i})$, $i = 1, 2, \cdots, t$. Now let M_0 be any point of $S - D$, let u be any arc from M_0 to M in $S - D$, and let $\alpha = uau^{-1}$. Then $h(\alpha)$ is gotten from $h(a)$ by a one-to-one mapping from $f^{-1}(M)$ onto $f^{-1}(M_0)$. Hence we have

LEMMA T1. *The canonical decomposition of $h(\alpha)$ into disjoint cycles consists of cycles of orders $r_1, r_2, \cdots, r_t$.*

Now let $P = P_1, P_2, \cdots, P_q, P_\infty$ be a labelling of the points of D.

Let a_i be the positively oriented boundary of a small circle A_i around P_i $(i=1,2,\cdots,q)$, let M_0 be a point in $S-D$ not on any line passing through any two of the points $P_1, P_2,\cdots,P_q$; let M_i be the points of intersection of M_0P_i with a_i, let u_i be the straight line from M_0 to M_i, and let $\alpha_i=u_ia_iu_i^{-1}$; let a_∞ be the positively oriented circumference of a large circle A_∞ containing $\alpha_1,\alpha_2,\cdots,\alpha_q$ (which is thus a *small* circle around P_∞), let u_∞ be a straight line from M_0 to a point M_∞ on a_∞ such that u_∞ such that u_∞ does not meet any of the α_i and let $\alpha_\infty=u_\infty a_\infty u_\infty^{-1}$. Arrange the labelling of the P_i so that $u_1,u_2,\cdots,u_q,u_\infty$ are consecutive lines through M_0. (The reader may draw a diagram.) Then it can easily be seen that

LEMMA T2. *α_∞ is homotopic to $\alpha_1\alpha_2\cdots\alpha_q$ (with M_0 fixed).*

Also the one-dimensional (cell) complex $J=\alpha_1\cup\alpha_2\cup\cdots\cup\alpha_q$ is a deformation retract of $R-D=S-D$ and $\pi_1(J,M_0)$ is the free group generated by $\alpha_1,\alpha_2,\cdots,\alpha_q$ (or loosely speaking: by $a_1,a_2,\cdots,a_q$) and hence we have

LEMMA T3. *$\pi_1(S-D,M_0)$ is the free group generated by $\alpha_1,\alpha_2,\cdots,\alpha_q$.*

Hence we have

PROPOSITION T3. (I) *$\pi_1(S-(q+1)$ points) is the free group F_q on q generators. In particular* (II) *$\pi_1(S-2$ points) is infinite cyclic and* (III) *$\pi_1(S-3$ points) is the free group F_2 on two generators.*

Corollary. A proof of Schreier's theorem. By Proposition 4, $S-3$ points can be covered by $S-(q+1)$ points for (arbitrarily) large q, hence $F_q=\pi_1(S-(q+1)$ points$)\subset\pi_1(S-3$ points$)=F_2$ for (arbitrarily) large q and hence $F_q\subset F_2$ for *all* q.

Moreover, by Proposition 4, for large q, $S_{q+1}=S-(q+1)$ points in a *finite* unramified covering of $S_3=S-3$ points; given a finite unramified regular covering Γ of S_{q+1} we may pass to the least regular unramified covering Γ^* of S_3 *dominating* Γ, then Γ^* is a finite covering of S_3 and the deck group of Γ over S_{q+1} is the homomorphic image of a subgroup of the deck group of Γ^* over S_3; since in Proposition 4 we could replace S_3 by S_n for any $n\geqq 3$, then denoting the free group on n generators by F_n, we have that $(F_{n-1})_{hsh}=(\pi_1(S_n))_{hsh}$ is complete. However if we observe that any finite group is isomorphic to a permutation group and that the symmetric group on any number of letters can be generated by two generators and that $(\pi_1(S_n))_{hs}\supset(\alpha_1(S_3))_{hs}$ there results a stronger assertion, namely

PROPOSITION T4. *For* $n \geqq 3$, $(\pi_1(S - n \textit{ points}))_{hs}$ *is complete.*

Now let L^* be a least normal extension of K containing L, let G be the galois group of L^*/K, let $[L^*:K] = n^*$. Let T^*, f^*, E^*, h^*, $H^*(X_0)$, $Q^*_1, Q^*_2, \cdots, Q^*_{t^*}$, $r^*_1, r^*_2, \cdots, r^*_{t^*}$ be the entities gotten from T, F, E, h, $H(X_0)$, $Q_1, Q_2, \cdots, Q_t$, $r_1, r_2, \cdots, r_t$ respectively by replacing L by L^*. Since L^*/K is normal, $r^*_1 = r^*_2 = \cdots = r^*_{t^*}$, let r^* be this common value. Let B^*_i be the connected component of $f^{*-1}(A_1)$ containing Q^*_i.

Let X_0 be any point of $S - D$. Recall that $H(X_0)$ is a permutation group of $f^{-1}(X_0)$; it is called the monodromy group of T over S. It is well-known that $H(X_0)$ is isomorphic to G; a classical proof can be found in any older treatise, secondly a modernistic proof in terms of associated principal bundles [S2] can be easily reconstructed, and thirdly the required isomorphism x of G onto $H(X_0)$ may be obtained thus: by the approximation theorem for valuations, we can find ξ in L whose values at the various points of $f^{-1}(X_0)$ are distinct, then for e in $H(X_0)$ define $x^{-1}(e)$ by setting $Y[x^{-1}(e)\xi] = e(Y)[\xi]$ for all Y in $f^{-1}(X_0)$ (if we replace the points of $f^{-1}(X_0)$ by their associated places, instead of the approximation theorem of valuations it would be enough to use the independence of places), observe that then for any $\eta \in L$, $g \in G$ and $Y \in f^{-1}(X_0)$ we have $Y[g(\eta)] = (x(g)Y)[\eta]$.

Replacing L by L^* and X_0 by M_0, we obtain an onto isomorphism $x^*: G \to H^*(M_0)$. Let $\bar{V}$ and V be the groups of fibre preserving (over S) autohomeomorphisms respectively of $T^* - E^*$ and T^*; by continuity, extension and restriction give an isomorphism between $\bar{V}$ and V. Since $T^* - E^*$ is a regular covering of $S - D$, if we fix a point N^*_0 in $f^{*-1}(M_0)$ we obtain a unique onto isomorphism $y^*: H^*(M_0) \to \bar{V}$ as follows: let $e \in H^*(M_0)$ and $Y^* \in T^* - E^*$ be given; let $X = f^*(Y^*)$, fix a loop β in $S - D$ at M_0 with $h^*(\beta) = e$ and fix an arbitrary arc δ^* in $T^* - E^*$ from Y^* to N^*_0 and let $\gamma = f^*(\delta)$, then $[y^*(e)][Y^*] = [h^*(\gamma\beta\gamma^{-1})](Y^*)$. Now y^* gives an onto isomorphism: $H^*(M_0) \to V$ which we again denote by y^*. Thus we have an onto isomorphism $y^*x^*: G \xrightarrow{x^*} H(M_0) \xrightarrow{y^*} V$; observe that for $g \in G$ and $Y^* \in T^*$ we simply have $[y^*x^*(g)](Y^*) = g(Y^*)$, ($Y^*$ is a valuation of L^*).

Let v_1 be the unique arc in $T^* - E^*$ starting from N^*_0 lying above u_1 and let N^*_1 be the point of v_1 lying above M_1, then $N^*_1 = [h^*(u_1)](N^*_0)$. Let B^*_i be the connected component of $f^{*-1}(A_1)$ containing N^*_1. Let $\mu = u_1^{-1}\alpha_1 u_1$, then $y^*(h^*(\alpha_1))(N^*_1) = h^*(\mu)(N^*)$. Now $\mu = u_1^{-1}\alpha_1 u_1 = u_1^{-1}u_1 a_1 u_1^{-1} u_1 = a_1$ and hence $y^*(h^*(\alpha_1))(N^*_1) = h^*(a_1)(N^*_1) \in B^*_i$. Therefore $y^*(h^*(\alpha_1))(Q^*_i) = Q^*_i$. By Lemma T1 the canonical decomposition of $h^*(\alpha_1)$ consists of r^*-cycles and hence the order of $h^*(\alpha_1)$, i.e., the order of $y^*(h^*(\alpha_1))$ is r^*. Let g_1 be the element of G which goes into $y^*(h^*(\alpha_1))$ under the isomorphism y^*x^*, then $g_1 = x^{*-1}y^{*-1}y^*h^*(\alpha_1) = x^{*-1}(\alpha_1)$, g_1 is of order r^* and g_1 maps the valuation Q^*_i of L^* onto itself, since the splitting group of Q^*_i over P_1 is of order r^*, g_1 must generate this group.

Similarly for $i = 1, 2, \cdots, q, \infty$ if we let $g_i = x^{*-1}(\alpha_i)$, there exists a valuation $\bar{Q}^*_i$ of L^* are lying above P_i such that g_i generates the splitting group of $\bar{Q}^*_i$ over P_i. Now suppressing the bar over $\bar{Q}^*_i$ and observing that the splitting groups of all the points of T^* lying above a given point of S form a complete conjugate set of subgroups of G, we conclude by Lemmas T2 and T3 the following

THEOREM T. *Let k be an algebraically closed field of characteristic zero having the cardinality of the continuum, let K be a simple transcendental extension of k, let L^* be a finite normal extension of K and let G be the galois group of L^*/K. Let $P_1, P_2, \cdots, P_{q+1}$ be the valuation of L^* lying above P_1. Then there exist valuations $Q^*_2, Q^*_3, \cdots, Q^*_{q+1}$ of L^* lying above $P_2, P_3, \cdots, P_{q+1}$ respectively and a generator g_i of the splitting group of Q^*_i over P_i for $i = 1, 2, \cdots, q+1$ such that* (I) $g_1 g_2 \cdots g_{q+1} = 1$ *and any q of the g_i generate G. In particular* (II) *the splitting groups of any q of the $q+1$ points Q^*_i (over the corresponding points P_i) generate G and hence a fortiori* (III) *the splitting groups of all the $q+1$ points Q^*_i generate G.*

Now observe that the order of $H(M_0)$ = order of $G = [L^*:K] = n^*$ ond fixe loops $\gamma_1, \gamma_2, \cdots, \gamma_{n^*}$ in $S - D$ at M_0 such that the elements $e_1 = h(\gamma_1), e_2 = h(\gamma_2), \cdots, e_{n^*} = h(\gamma_{n^*})$ are all distinct and hence these are all the elements of $H(M_0)$. Since $T^* - E^*$ is an unramified covering of $T - E$ it follows that $h^*(\gamma_1), h^*(\gamma_2), \cdots, h^*(\gamma_{n^*})$ are all distinct and hence these are all the elements of $H^*(M_0)$. Recall that N^*_0 is a fixed point in $f^{*-1}(M_0)$. Let $N^*_i = h^*(\gamma_i)N^*_0$. Then $N^*_1, N^*_2, \cdots, N^*_{n^*}$ are all distinct and these are all the points of $f^{*-1}(M_0)$. Now

$$h^*(\gamma_i\gamma_j)N^*_0 = h^*(\gamma_j)[h^*(\gamma_i)N^*_0] = h^*(\gamma_j)N^*_i$$

and hence if we identify $\gamma_1, \gamma_2, \cdots, \gamma_{n^*}$ respectively with $e_1, e_2, \cdots, e_{n^*}$ and $N^*_1, N^*_2, \cdots, N^*_{n^*}$ respectively with $h^*(\gamma_1), h^*(\gamma_2), \cdots, h^*(\gamma_{n^*})$, there results the following: $H^*(M_0)$ is the right regular representation of $H(M_0)$. Hence by Lemma T1: [least comon multiple of $r_1, r_2, \cdots, r_t$] = [order of $h(({}_1)$] = [the order of a cycle in the canonical decomposition of $h^*(\gamma_1)$] = r^*. Hence we may state

PROPOSITION T5. *Let K/k and L^* be as in Theorem* T *and let L be a field between K and L^* such that L^* is a least normal extension of K containing L. Let P be a valuation of K/k, let $Q_1, Q_2, \cdots, Q_t$ be all the valuations of L lying above P and let Q^* be any valuation of L^* lying above P. Then $d(Q^*:P) =$ the least common multiple of $d(Q_1:P), d(Q_2:P), \cdots, d(Q_t:P)$.*

8. Appendix. We put together here the proofs of some of the lemmas we have used.

LEMMA A1. *Let $G(Z) = Z^g + G_1(X)Z^{g-1} + G_2(X)Z^{g-2} + \cdots + G_g(X)$ with $G_i(X) \in k[[X]] = k[[X_1, X_2, \cdots, X_t]]$ where k is an arbitrary field. Assume that $| G_i(X) |_X \geqq i$ for $i = 1, 2, \cdots, g-1$ and $| G_g(X) |_X = g-1$. Then $G(Z)$ is irreducible in $k[[X]][Z]$.*

Proof. Suppose if possible that $G(Z) = H(Z)K(Z)$ with

$$H(Z) = Z^h + H_1(X)Z^{h-1} + H_2(X)Z^{h-2} + \cdots + H_h(X), H_i(X) \in k[[X]];$$

$$K(Z) = Z^k + K_1(X)Z^{k-1} + K_2(X)Z^{k-2} + \cdots + K_k(X), K_i(X) \in k[[X]].$$

Let $H^*(Z,X)$ and $K^*(Z,X)$ be the leading forms respectively of $H(Z)$ and $K(Z)$ considered as elements of $k[[X,Z]]$. Then $H^*(Z,X)$ and $K^*(Z,X)$ are in $k[[X]][Z]$. Let $G^*(X)$ be the leading form of $G_g(X)$. Since

$$| G_g(X) |_{X,Z} = g-1 < g = \min[| Z^g |_{X,Z}, \\ | G_1(X)Z^{g-1} |_{X,Z}, \cdots, | G_g(X) |_{X,Z}],$$

$G^*(X)$ is also the leading form of $G(Z)$ as an element of $k[[X,Z]]$. Hence $H^*(Z,X)K^*(Z,X)$ are in $[[X]]$. Hence $H^*(Z,X) =$ leading form of $H_h(X)$, and $K^*(Z,X) =$ leading form of $K_k(X)$. Hence $h = | Z^h |_{X,Z} > | H_h(X) |_{X,Z} = | H_h(X) |_X$ so that $h-1 \geqq | H_h(X) |_X$. Similarly $k-1 \geqq | K_k(X) |_X$. Therefore

$$g-2 = h+k-2 = | H_h(X) |_X + | K_k(X) |_X = | H_h(X)K_k(X) |_X \\ = | G_g(X) |_X = g-1.$$

This is a contradiction and the lemma is established.

LEMMA A2. *Let $F(Z) = Z^{p+1} + x^{p-1}Z + x^{p+1} \in k[[x]][Z]$ and let $H(Z) = Z^p + x^2Z^{p-1} + x^{p-1}$ where k is an algebraically closed field of characteristic $p \neq 0$. The galois groups of $F(Z)$ and $H(Z)$ over $k((x))$ are isomorphic as permutation groups.*

Proof. By equation (7) of Section 2, $F(Z) = G(Z)(Z + ux^2)$, where $u \in k[[x]]$ and $G(Z)$ is an irreducible monic polynomial in $k[[x]][Z]$; the isomorphism in the statement of the lemma is to be interpreted as an isomorphism between the galois groups of $G(Z)$ and $H(Z)$ over $k((x))$ as premutation groups.

Let $Z_1 = Z + ux^2$, $F_1(Z_1) = F(Z)$, $H_1(Z_1) = G(Z)$. Then

$$\begin{aligned} F_1(Z_1) = F(Z) = F(Z_1 - ux^2) &= (Z_1 - ux^2)[(Z_1 - ux^2)^p + x^{p-1}] + x^{p+1} \\ &= (Z_1 - ux^2)[Z_1^p - u^p x^{2p} + x^{p-1}] + x^{p+1} \\ &= Z_1^{p+1} - ux^2 Z_1^p + x^{p-1}(1 - u^p x^{p+1}) Z_1 + F_1(0) \end{aligned}$$

$= Z_1[Z_1^p - ux^2 Z_1^{p-1} + x^{p-1}(1 - u^p x^{p+1})]$, since $F_1(0) = F(-ux^2) = 0$.

Therefore

$$H_1(Z_1) = Z_1^p + dx^2 Z_1^{p-1} + ex^{p-1},$$

where d and e are units in $k[[x]]$. Let $Z_1 = Z^*\delta_1$ and $x = x^*\delta_2$ where δ_1 and δ_2 are units in $k[[x]]$ to be chosen. Now

$$\begin{aligned} H_1(Z_1) &= \delta_1^p Z^{*p} + d\delta_1^{p-1}\delta_2^2 x^{*2} Z^{*p-1} + e\delta_2^{p-1} x^{*p-1} \\ &= \delta_1^p (Z^{*p} + d\delta_1^{-1}\delta_2^{-2} Z^{*p-1} + e\delta_1^{-p}\delta_2^{p-1} x^{*p-1}). \end{aligned}$$

We want

$$(1) \qquad d\delta_1^{-1}\delta_2^2 = 1 \text{ and } e\delta_1^{-p}\delta_2^{p-1} = 1$$

i.e.,

$$(2) \qquad \delta_1 = d\delta_2^2 \text{ and } \delta_2^{p-1} = e^{-1}\delta_1^p.$$

Equations (2) imply: $\delta_2^{p-1} = e^{-1} d^p \delta_2^{2p}$ which in turn implies $\delta_2^{p+1} = ed^{-p}$. Now $(ed^{-p})(0) = e(0)d(0)^{-p} = e(0)u(0)^{-p} = 1$. Sincs $p + 1 \not\equiv 0 \pmod p$, by Hensel's Lemma, we can find a unit δ_2 in $k[[x]]$ with $\delta_2(0) = 1$ and $\delta_2^{p+1} = ed^{-p}$. Substituting in the first equation of (2), we let $\delta_1 = d\delta_2^2$. Then the required equations (1) are satisfied and we have

$$\delta_1^{-p} G(Z) = \delta_1^{-p} H_1(Z_1) = Z^{*p} + x^{*2} Z^{*p-1} + x^{*p-1}.$$

LEMMA A3. *Let k be an arbitrary field, let y be a transcendental over k and let u_1, u_2, u_3 be any three distinct valuations of $k(y)/k$ rational over k. Then there exists a generator z of $k(y)/k$ such that u_1: $z = 0$, u_2: $z = 1$ and u_3: $z = \infty$. Hence if v_1, v_2, v_3 are any three distinct rational valuations of $k(y)/k$, then there exists a k-automorphism of $k(y)$ which maps u_i onto v_i for $i = 1, 2, 3$.*

Proof. If u_3 is not $y = \infty$ then there exists unique c in k such that

$u_3(y-c)=1$, let $y'=1/(y-c)$; then $k(y')=k(y)$ and u_3 is $y'=\infty$; hence to begin with, we may assume that u_3 is $y=\infty$. Then there exists a unique d in k with $u_1(y-d)=1$; replacing y by $y-d$ we may assume that u_1 is $y=0$. Then there exists a unique e in k with $e\neq 0$ and $u_2(y-e)=1$. It is enough to take $z=(1/e)y$.

LEMMA A4. *Let G be a finite group and p a prime number. Assume that G has only one p-sylow subgroup S (which is therefore a normal subgroup of G). Let H be a given subgroup of G and let $[G:H]=n=mp^a$ with $m\not\equiv 0(p)$.*[2] *Then $[G:HS]=m$, i.e., $[HS:H]=p^a$, and HS is the only such subgroup of G containing H. If G/S is abelian, then HS is a normal subgroup of G.*

Proof. Let $[H:1]=n'=m'p^{a'}$ with $m'\not\equiv 0(p)$. Then $[G:1]=nn'=mm'p^{a+a'}$ and $mm'\not\equiv 0(p)$ so that $[S:1]=p^{a+a'}$. Let S^* be a p-sylow subgroup of H; then the order of S^* is $p^{a'}$. Since S is the only p-sylow subgroup of G, $S^*\subset S$ (Theorem 4, p. 107 of [Z]) and hence $S^*=S\cap H$. Therefore HS/S is isomorphic to H/S^* and hence $[HS:S]=[H:S^*]=m'$ so that $[G:HS]=[G:S]/[HS:S]=(mm')/m'=m$. If G^* is a subgroup of G containing H such that $[G:G^*]=m$, then $[G^*:1]=m'p^{a+a'}$ and hence the unique p-sylow subgroup S of G must be contained in G^* and hence $G^*\supset HS$; since $[G:G^*]=m=[G:HS]$ we must have $G^*=HS$. If G/S is abelian, HS/S is a normal subgroup of G/S and hence HS is a normal subgroup of G.

LEMMA A5. *Let $E=k((x))$ where k is algebraically closed of characteristic p. Let E^* be a finite separable algebraic extension of E, let $[E^*:E]=n$ and $n=mp^a$ with $m\not\equiv 0(p)$ if $p\neq 0$ and $n=m$ if $p=0$. Then $x^{1/m}\in E^*$ so that $[E^*:F]=p^a$ and $[F:E]=m$ where $F=k((x^{1/m}))=E(x^{1/m})$. Let E^*_1 be a root field of X^g-x^h over E^* where g and h are integers, g is positive and $g\not\equiv 0(p)$ if $p\neq 0$; let E_1 be the root field of X^g-x^h over E in E^*_1; let $q=(g,h)$, $g_1=g/q$, $q^*=(g_1,n)$, $N^*=g_1/q^*$ and $N=n/q^*$. Then $[E^*_1:E_1]=N$ and $[E^*_1:E^*]=N^*$.*

Proof. For $p=0$, everything follows from well-known theorems, so assume $p\neq 0$. Let E' be a galois extension of E^* containing E, let G be the galois group of E' over E and let H be the galois group of E' over E^*. Then G contains a unique p-sylow subgroup S and G/S is cyclic (see [K]). Let F be the fixed field of HS. Then by Lemma A4, $[F:E]=m\not\equiv 0(p)$

---

[2] For a subgroup H of a finite group G we shall denote the index of H in G by $[G:H]$.

and hence $F = E(x^{1/m})$. To prove the second part, let z be a root of $X^g - x^h$. Then $E^*_1 = E^*(z)$ and multiplying z by a root of unity, we may assume that $z^{g_1} = x^{h_1}$ where $h_1 = h/q$. Then $(g_1, h_1) = 1$ and hence (as in Section 5 of [A2]) we may arrange matters so that $h_1 = 1$. Since by the first part we know that $x^{1/m}$ is the lowest positive power of x in E^* and since $q^* = (g_1, n) = (g_1, m)$, we conclude that $X^{N^*} - x^{1/q}$ is the minimal polynomial of z over E^*. Therefore $[E^*_1 : E^*] = N^*$. Hence $[E^*_1 : E_1] = [E^*_1 : E][E_1 : E]^{-1} = [E^*_1 : E^*][E^* : E][E_1 : E]^{-1} = N^* n g_1^{-1} = g_1 q^{*-1} n g_1^{-1} = N$.

COLUMBIA UNIVERSITY.

REFERENCES.

[A1] S. Abhyankar, "On the ramification of algebraic functions," *American Journal of Mathematics*, vol. 77 (1955), pp. 575-592.

[A2] ———, "Local uniformization on algebraic surfaces over ground fields of characteristic $p \neq 0$," *Annals of Mathematics*, vol. 63 (1956), pp. 491-526.

[A3] ———, "On the ramification of algebraic functions, Part II: Unaffected equations for characteristic two," forthcoming in the Transactions of the American Mathematical Society.

[C] C. Chevalley, *Introduction to the theory of algebraic functions of one variable*, New York, 1951.

[D] M. Deuring, "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper," *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, vol. 14 (1941), pp. 197-272.

[H] H. Hasse, "Existenz separabler zyklischer unverzweigter Erweitungskörper vom Primzahlgrade p über elliptnschen Funktionenkörpern der Charakteristic p," *Crelle Journal*, vol. 172 (1934), pp. 77-85.

[K] W. Krull, "Galoissche Theorie bewerteter Körper," *Sitzungsberichte der Bayerschen Akademie des Wissenschaften*, 1930, pp. 225-238.

[L1] S. Lang, "Algebrais groups over finite fields," *American Journal of Mathematics*, vol. 78 (1956), pp. 555-563.

[L2] ———, "Sur le séries L d'une variété algébrique," *Bulletin de la Société Mathematique de France*, vol. 84 (1956), pp. 385-407.

[LS] ———, and J.-P. Serre, "Sur les revêtments non ramifiés des variétés algébriques." *American Journal of Mathematics*, vol. 79 (1957), pp. 319-330.

[O] A. Ostrowski, "Untersuchungen zur arithmetischen Theorie der Körper," *Mathematische Zeitschrift*, vol. 39 (1934), pp. 269-404.

[S1] J.-P. Serre, "Sur la topologie des variétés algébrique en characteristic p," Symposium of algebraic topology, Mexico (1956).

[S2] N. Steenrod, *The topology of fibre bundles*, Princeton, 1951.

[V] B. L. van der Waerden, *Modern Algebra*, vol. I, New York, 1949.

[Z] H. Zassenhaus, *The theory of groups*, New York, 1949.

VARIATIONAL METHODS IN ENTIRE FUNCTIONS.*

By R. P. Boas, Jr. and A. C. Schaeffer.[1]

1. Introduction. Consider the class of entire functions $f(z)$ of exponential type τ, such that $|f(x)| \leqq M$ for all real x. We ask for the smallest $A_n(\tau)$ such that

$$|\sum_{k=0}^{n} f'(k+x)| \leqq A_n(\tau) M \tag{1.1}$$

for all f in the class. By S. Bernstein's famous theorem (see, e.g., [2], p. 206), $A_n(\tau)$ does not exceed $(n+1)\tau$. In another paper [3] we have shown that $A_n(\tau) \leqq \pi$ when $\tau \leqq \pi$; the example $f(z) = \sin \pi z$ shows that this estimate is sharp when n is even, but we have shown that it is not sharp when n is odd; in particular, $A_1(\pi) < 8/\pi < \pi$. In the present paper we attack the problem of finding the best possible $A_n(\tau)$. It is not difficult to show that, for a given x_0, there is a function $f_0(z)$ for which (1.1) becomes an equality. We shall show by variational methods that $f_0(z)$ satisfies a differential equation which is generally hyperelliptic; the determination of $A_n(\tau)$ is then reduced to the investigation of solutions of this differential equation. We shall develop the variational methods for a more general case, since they can be used for other questions in the theory of entire functions. There are analogous questions for polynomials, which have been investigated by Chebyshev [4] and Zolotarev [6].

For $n=1$ (that is, for $|f'(x)+f'(x+1)|$) we can give the extremal function fairly explicitly for every τ, although for some values of τ it is expressed in terms of elliptic integrals and we do not obtain an explicit formula for $A_n(\tau)$. A detailed statement is given in Section 10. As simpler applications of the variational method we determine the maximum of $|\lambda f(x) + f''(x)|$ (§ 8) and of $|f'(x) - f'(x+1)|$ (§ 9).

---

* Received February 18, 1957.

[1] This represents work done by Boas with partial support of the National Science Foundation and by Schaeffer under Contract N7 onr-28507 with the Office of Naval Research.

2. The variational problem. Let $\mathscr{L}$ be the linear functional defined by

$$\mathscr{L}(f) = \sum_{\nu=1}^{m} \sum_{j=0}^{n_\nu} \alpha_\nu^{(j)} f^{(j)}(x_\nu), \tag{2.1}$$

where $x_1, \cdots, x_m, \alpha_\nu^{(j)}$ are given real numbers, with the x_ν all different. We suppose that $\alpha_\nu^{(n_\nu)} \neq 0$, and that $n_\nu > 0$ for at least one ν. We call

$$l = n_1 + n_2 + \cdots + n_m + m$$

the order of the functional $\mathscr{L}$. Thus $f'(\frac{1}{2}) + f'(-\frac{1}{2})$ is a functional of order 4.

We wish to investigate the existence and properties of the entire function $f(z)$, of exponential type τ, bounded by 1 on the real axis, for which $|\mathscr{L}(f)|$ is largest. We may, without loss of generality, restrict our attention to functions which are real for real z. For, if θ is real, we have $e^{i\theta} f(z) = f_1(z) + i f_2(z)$, where f_1 and f_2 are entire functions of exponential type τ, real for real z, and bounded by 1 on the real axis. Since $\mathscr{L}(e^{i\theta} f) = e^{i\theta} \mathscr{L}(f)$, we can choose θ so that $\mathscr{L}(e^{i\theta} f) = |\mathscr{L}(f)|$, and so $\mathscr{L}(f_1) = |\mathscr{L}(f)|$. Hence the maximum of $|\mathscr{L}(f)|$ is attained, if at all, for an f which is real on the real axis, and for which $\mathscr{L}(f) \geqq 0$.

Let $\mathfrak{F}_\tau$ denote the class of entire functions f of exponential type τ which are real for real z and satisfy $|f(x)| \leqq 1$ for $-\infty < x < \infty$. (We emphasize that in our terminology $\mathfrak{F}_\tau$ includes all functions of order 1 and type not exceeding τ, as well as all entire functions of order less than 1.)

LEMMA 2.2. *If τ and a linear functional $\mathscr{L}$ are given then $M = \sup |\mathscr{L}(f)|$, $f \in \mathfrak{F}_\tau$, is finite, positive, and attained.*

It is well known (cf. [2], p. 83) that if $f \in \mathfrak{F}_\tau$ then

$$|f(x + iy)| \leqq e^{\tau |y|}, \tag{2.3}$$

so that $\mathfrak{F}_\tau$ is a normal family. Bernstein's theorem shows that M is finite, and so it is attained for some element of $\mathfrak{F}_\tau$. Finally, M is positive because we can readily exhibit elements of $\mathfrak{F}_\tau$ for which $f^{(j)}(x_\nu) = 0$ for all j and ν entering the definition of $\mathscr{L}$, except $\nu = m$, $j = n_m$. Indeed, we can have $\mathscr{L}(f) \neq 0$ for an f such that $f(x) \to 0$ as $|x| \to \infty$. To verify this, let $p(z)$ be a polynomial with real coefficients which has a zero of order n_1 at x_1 and zeros of order $n_\nu + 1$ at x_ν for $\nu \neq 1$, so that $p(z)$ is of degree $l - 1$. Then

$$f(z) = c\{[\sin \epsilon(z - x_1)]/(z - x_1)\}^l p(z)$$

has the desired property if ϵ and c are small enough positive constants, since $f^{(k)}(z_\nu) = 0$ for $k = 0, 1, \cdots, n_\nu$ and $\nu = 2, 3, \cdots, m$, while $f^{(n_1)}(x_1) \neq 0$.

Our central result is as follows.

THEOREM 1. *The element* f *of* $\mathfrak{F}_\tau$ *for which*

$$\mathcal{L}(f) = \sup \mathcal{L}(g), \qquad g \in \mathfrak{F}_\tau, \tag{2.4}$$

is unique, and either constant[2] *or of order* 1 *and type* τ *(i.e., not of exponential type less than* τ*). If not constant, it satisfies a differential equation*

$$\{f'(z)\}^2/(1-\{f(z)\}^2) = \tau^2\{p(z)\}^2/q(z), \tag{2.5}$$

where $p(z)$ *and* $q(z)$ *are monic polynomials with real coefficients; the degree of* $p(z)$ *is at most* $l-2$ *and the degree of* $q(z)$ *is precisely twice that of* $p(z)$*. The zeros of* $q(z)$ *are simple and not real, and* $q(x) \geqq \{p(x)\}^2$ *for real* x*, with equality at some point if and only if* $p(z) \equiv q(z) \equiv 1$.

This result may be formulated in somewhat different language. If $x_1, \cdots, x_m$ are given distinct real numbers and $n_1, \cdots, n_m$ are nonnegative integers, then

$$(f(x_1), f'(x_1), \cdots, f^{(n_1)}(x_1), \cdots, f^{(n_m)}(x_m))$$

is a point in l-dimensional Euclidean space, and we say that this point belongs to $f(z)$. Let E be the set of points belonging to the elements of $\mathfrak{F}_\tau$. The content of Lemma 2.2 is that E is closed and bounded and contains a point other than the origin. Furthermore, E is convex since $\mathfrak{F}_\tau$ is convex. Theorem 1 shows that a boundary point of E belongs to a unique element of $\mathfrak{F}_\tau$ and this function satisfies (2.5).

When all the n_ν are zero in (2.1), so that

$$\mathcal{L}(f) = \sum_{\nu=1}^{m} \alpha_\nu f(x_\nu),$$

Theorem 1 fails, but similar results can be obtained; see Section 15.

3. Lemmas for Theorem 1.

If $f(z) \in \mathfrak{F}_\tau$ the real zeros of $1-f(z)^2$ are of even order and the imaginary zeros occur in conjugate pairs. Let $\lambda_1, \lambda_2, \cdots$ be the distinct real points where $1-f(z)^2 = 0$. We wish to consider the imaginary zeros of $1-f(z)^2$ together with the real zeros whose orders exceed 2. These are the zeros of the entire function

$$(1-f(z)^2)/\{\prod(1-z/\lambda_n)^2 e^{2z/\lambda_n}\}, \tag{3.1}$$

---

[2] We do not know of any example in which the extremal function is constant, but since the possibility causes little difficulty in any particular case, we have not attempted to exclude it.

and there are either a nonnegative even number of them, or infinitely many. If some $\lambda_\nu = 0$, the denominator contains the term z^2 and the product extends over $n \neq \nu$.

LEMMA 3.2. *If* (3.1) *has at least* $2k$ *zeros then there is a function* $g(z)$ *in* $\mathfrak{F}_\tau$ *which has a zero at each* λ_n *and is such that* $x^k g(x)$ *is bounded for real* x.

The zeros of (3.1) are either real or occur in conjugate pairs. Let $p(z)$ be a polynomial of degree $2k$, with real coefficients, which is nonnegative for real z and whose zeros are among the zeros of (3.1). Then $F(z) = \{1 - f(z^2\}/p(z)$ is an entire function of exponential type 2τ, real and nonnegative for real z, and it has a zero of order at least 2 at each λ_ν. Furthermore, $F(x)$ is bounded for real x (indeed, it is $O(x^{-2k})$ as $|x| \to \infty$). Then if z_n are the zeros of $F(z)$, it follows ([2], p. 86) that $\sum |\Im(1/z_n)| < \infty$. This implies ([2], p. 125) that there is an entire function $\phi(z)$ of exponential type τ such that $F(z) = \phi(z)\{\phi(z^*)^*\}$, where the star denotes the complex conjugate. Then $\phi(x) = O(|x|^{-k})$ as $|x| \to \infty$ and $\phi(\lambda_\nu) = 0$. Finally, $g(z) = c\{\phi(z) + \phi(z^*)^*\}$ has all the properties stated in Lemma 3.2 if c is a sufficiently small positive constant.

LEMMA 3.3. *Let* f *be an element of* $\mathfrak{F}_\tau$, *not constant, satisfying* (2.4). *Then* $|f(x)| = 1$ *for at least one real* x; *and if* $F(z) \in \mathfrak{F}_\tau$ *and* F *has a zero at each of the distinct real points where* $f(x) = \pm 1$, *then* $\mathcal{L}(F) = 0$.

We shall prove the second part of Lemma 3.3 here only under the additional hypothesis

$$\lim_{x \to +\infty} F(x) = 0. \tag{3.4}$$

After obtaining more information about the extremal function $f(z)$ we shall prove the lemma in full generality.

Consider the function $g_\epsilon(z) = f(z) + \epsilon F(z)$, where ϵ is real. Then $g_\epsilon(z)$ is entire and of exponential type τ. We begin by showing that if $F(z)$ is any element of $\mathfrak{F}_\tau$ and

$$\sup_{-\infty < x < \infty} |f(x) + \epsilon F(x)| = 1 + o(\epsilon), \qquad \epsilon \to 0, \tag{3.5}$$

where ϵ is real, then $\mathcal{L}(F) = 0$. For, let $0 < \rho < 1$. According to (3.5), if $|\epsilon| < \epsilon_0(\rho)$, the function

$$\psi_\epsilon(z) = \{f(z) + \epsilon F(z)\}/\{1 + |\epsilon|\rho\}$$

belongs to $\mathfrak{F}_\tau$. If $\mathscr{L}(F) \neq 0$ then

$$\mathscr{L}(\psi_\epsilon) = \{\mathscr{L}(f) + \epsilon\mathscr{L}(F)\}/\{1 + |\epsilon|\rho\}.$$

Choose ρ so that $\rho\mathscr{L}(f) < |\mathscr{L}(F)|$, then ϵ so that $|\epsilon| < \epsilon_0(\rho)$ and so that $\epsilon\mathscr{L}(F) > 0$. We then have $\mathscr{L}(\psi_\epsilon) > \mathscr{L}(f)$, contradicting the maximizing property assumed for f. Hence $\mathscr{L}(F) = 0$.

To establish the first part of Lemma 3.3, suppose $|f(x)| < 1$ for all finite x. We can find an F in $\mathfrak{F}_\tau$ satisfying (3.4) and with $\mathscr{L}(F) \neq 0$ as in the proof of Lemma 2.2. Write $g_\epsilon(x) = f(x) + \epsilon F(x)$. Let δ be a positive number and let $x_0 = x_0(\delta)$ be so large that $|F(x)| \leqq \delta$ for $|x| \geqq x_0$. Then

$$(3.6) \qquad |g_\epsilon(x)| \leqq 1 + \delta|\epsilon|, \qquad |x| \geqq x_0.$$

Since $|f(x)| < 1$ in $|x| \leqq x_0$ we have $|g_\epsilon(x)| < 1$ in $|x| \leqq x_0$ if ϵ is small enough, so the inequality in (3.6) holds for all x. Hence (3.5) holds and we infer that $\mathscr{L}(F) = 0$, a contradiction.

Now suppose that F satisfies (3.4) and has a zero at each of the distinct real points where $f(x) = \pm 1$. Since F satisfies (3.4) we have (3.6) again, and (3.5) follows unless $|f(x)| = 1$ at some point in $|x| \leqq x_0$. In the latter case there are only a finite number of such points. Let λ be one of these points. Then there is an interval I with center at λ such that

$$|f(x)| \leqq 1 - h(x-\lambda)^{2\mu}$$

in I, where $h > 0$ and μ is a positive integer. Since $F(\lambda) = 0$, Bernstein's theorem shows that $|F(x)| \leqq \tau|x-\lambda|$, so

$$|g_\epsilon(x)| \leqq 1 - h(x-\lambda)^{2\mu} + \epsilon\tau|x-\lambda|$$

in I. The maximum of the right-hand side does not exceed $1 + B\epsilon^{1+1/(2\mu-1)}$, where B depends only on h, τ and μ. Thus $|g_\epsilon(x)| \leqq 1 + o(\epsilon)$ in the intervals I, while $|g_\epsilon(x)| \leqq 1$ for small ϵ outside these intervals. These facts, together with (3.6), establish (3.5). This implies, as we saw, that $\mathscr{L}(F) = 0$. This establishes the second part of Lemma 3.3 under the hypothesis (3.4).

LEMMA 3.7. *Given a set of distinct real points* $\lambda_1, \lambda_2, \cdots$, *if there is an element* $G(z)$ *of* $\mathfrak{F}_\tau$, *not vanishing identically, such that* $G(\lambda_\nu) = 0$ *and* $G(x) = O(|x|^{1-l})$ *as* $|x| \to \infty$, *then there is an element* $g(z)$ *of* $\mathfrak{F}_\tau$ *such that* $g(\lambda_\nu) = 0$ *and* $\mathscr{L}(g) \neq 0$. *If* $G(x) = O(|x|^{-l})$ *as* $|x| \to \infty$, *then, in addition,* $g(x) \to 0$ *as* $|x| \to \infty$.

If $G(z)$ has a zero at any of the points x_ν, let $G_1(z) = G(z)/p_1(z)$, where $p_1(z)$ is a polynomial with real coefficients whose zeros are in the intersection of $\{x_\nu\}$ and $\{\lambda_\nu\}$. If $G(z)$ has no zero at any x_ν let $G_1(z) = G(z)$. Then $G_1(z)$ is an entire function which has zeros at the λ_ν which are not in $\{x_\nu\}$. We have assumed that some $n_\nu > 0$; suppose for definiteness that $n_1 > 0$. Let $p_2(z)$ be a polynomial with real coefficients which has a zero of order n_1 at x_1 and zeros of order $n_\nu + 1$ at x_ν for $\nu \neq 1$. Then $p_2(z)$ is of degree $l - 1$. Define $g(z) = cG_1(z)p_2(z)$, where c is a real constant, not 0, but so small that $g \in \mathfrak{F}_\tau$. Then $g^{(k)}(x_\nu) = 0$ for $k = 0, 1, 2, \cdots, n_\nu$ and $\nu = 2, 3, \cdots, m$. Hence $\mathscr{L}(g) = \alpha_1^{(n_1)} g^{(n_1)}(x_1) \neq 0$. The hypothesis $G(x) = O(|x|^{1-l})$ makes $g(x)$ bounded; so $G(x) = O(|x|^{-l})$ makes $g(x) \to 0$ as $|x| \to \infty$.

The only place where we have used the fact that some $n_\nu > 0$ (i.e., that $\mathscr{L}(f)$ actually involves derivatives) is in the last part of the proof of Lemma 3.7. If all n_ν are 0, $g(x_1) \neq 0$, and in case x_1 happens to be a λ_ν we cannot complete the proof. Indeed, if all n_ν are 0 and all x_ν are λ_ν's we cannot have g in $\mathfrak{F}_\tau$ such that $g(\lambda_\nu) = 0$ and $\mathscr{L}(g) \neq 0$.

4. Proof of part of Theorem 1.

We prove part of Theorem 1, and then use this part to prove Lemma 3.3 without the additional hypothesis (3.4). Then we shall use Lemma 3.3 to complete the proof of Theorem 1.

Let $f(z)$, not a constant, belong to $\mathfrak{F}_\tau$ and maximize $\mathscr{L}$ in $\mathfrak{F}_\tau$. To show, first, that $f(z)$ is not of exponential type less than τ, suppose that it is of type $\gamma < \tau$. Let $0 < \epsilon < \tau - \gamma$ and define $\phi(z) = \{\sin \epsilon z\}/p(z)$, where $p(z)$ is a polynomial of degree l with real coefficients, whose zeros are among the zeros of $\sin \epsilon z$. If c is a sufficiently small positive number, $G(z) = cf'(z)\phi(z)$ belongs to $\mathfrak{F}_\tau$. If λ_ν are the distinct real points where $f(x) = \pm 1$ (there is at least one, by the part of Lemma 3.3 that has been established), Lemma 3.7 gives us a function g such that $g(\lambda_\nu) = 0$, $\mathscr{L}(g) \neq 0$, and $g(x) \to 0$ as $|x| \to \infty$. The special case of Lemma 3.3 which has already been proved now shows that $\mathscr{L}(g) = 0$, a contradiction. Hence f is not of type less than τ.

Again let f, not a constant, belong to $\mathfrak{F}_\tau$ and maximize $\mathscr{L}$ in $\mathfrak{F}_\tau$. We know that $1 - f(x)^2$ has at least one real zero; let the distinct points where $f(x) = \pm 1$ be $\lambda_1, \lambda_2, \cdots$. Then $f'(\lambda_\nu) = 0$. We shall show that $1 - f(z)^2$ has at most $2l - 2$ zeros besides its double zeros at the λ_ν, and that $f'(z)$ has at most $l - 1$ zeros besides its simple zeros at the λ_ν.

For, suppose $1 - f(z)^2$ has $2l$ additional zeros. Then the function (3.1) has at least $2l$ zeros. Let $g(z)$ be the function constructed in Lemma

3.2 with $k = l$. By Lemma 3.7 there is a function $g_1(z)$ which belongs to $\mathfrak{F}_\tau$ and has the properties

$$g_1(\lambda_\nu) = 0, \quad \mathcal{L}(g_1) \neq 0, \quad g_1(x) \to 0 \text{ as } |x| \to \infty. \tag{4.1}$$

This contradicts Lemma 3.3.

If $f'(z)$ has at least l zeros besides simple zeros at the λ_ν, let l of them be divided out; that is, write $G(z) = f'(z)/p(z)$, where $p(z)$ is a polynomial of degree l with real coefficients, such that $G(z) \in \mathfrak{F}_\tau$, with $G(\lambda_\nu) = 0$. By Lemma 3.7 there is a function $g_1(z)$ in $\mathfrak{F}_\tau$ with the properties (4.1). This again contradicts Lemma 3.3.

Thus there is a polynomial $P_1(z)$ of degree at most $2l - 2$ such that $\{1 - f(z)^2\}/P_1(z)$ has zeros of order 2 at each λ_ν, and no other zeros. There is also a polynomial $P_2(z)$ of degree at most $l - 1$ such that $f'(z)/P_2(z)$ has simple zeros at each λ_ν, and no other zeros. Hence

$$\phi(z) = \{f'(z)^2/(1 - f(z)^2)\} \cdot \{P_1(z)/P_2(z)^2\}$$

is an entire function with no zeros, taking real values on the real axis. It is of exponential type, as may be seen, for instance, from minimum modulus theorems ([2], p. 52). Hence $\phi(z)$ is of the form e^{az+b} with real a and b. Thus

$$f'(z)^2/P_2(z)^2 = e^{az+b}(1 - f(z)^2)/P_1(z).$$

The left-hand side is bounded on the real axis, and if $a \neq 0$ it must decrease exponentially either as $x \to +\infty$ or as $x \to -\infty$. This is impossible, since $f'(z) \not\equiv 0$ ([2], p. 69), so $a = 0$.

We thus have

$$f'(z)^2/(1 - f(z)^2) = \gamma p(z)^2/q(z), \tag{4.2}$$

where p is a polynomial of degree at most $l - 1$ and q is a polynomial of degree at most $2l - 2$, each with real coefficients and leading coefficient 1. We suppose that all common factors of p^2 and q have been cancelled. Since everything is real on the real axis and the left-hand side of (4.2) is positive, $\gamma > 0$. Thus

$$f'(z)/\{1 - f(z)^2\}^{\frac{1}{2}} = \gamma^{\frac{1}{2}} p(z)/\{q(z)\}^{\frac{1}{2}}.$$

Integrating this, we have

$$f(z) = \sin \psi(z), \tag{4.3}$$

where

$$\psi(z) = \gamma^{\frac{1}{2}} \int_0^z \{q(z)\}^{-\frac{1}{2}} p(w)\, du + \sin^{-1} f(0). \tag{4.4}$$

Since $f(z)$ is not of exponential type less than τ, we see that the degree of q is precisely twice that of p, and that $\gamma^{\frac{1}{2}} = \pm \tau$.

Since the rational function in (4.2) is in lowest terms, $p(z_0) \neq 0$ if z_0 is at least a double zero of $q(z)$. It now follows that $q(z)$ has only simple zeros. For, if z_0 is at least a double zero of $q(z)$, then $p(z_0) \neq 0$, and (4.4) shows that $|\psi(z)| \to \infty$ as $z \to z_0$. But $f(z) = \sin \psi(z)$ is regular at z_0.

Hence $q(z)$ has no real zeros, since everything in (4.2), except possibly $q(z)$, is nonnegative for real z. Thus $q(x) \geqq 0$ and any real zeros of q would have to be multiple.

Our next task is to show that $p(z)$ is of degree at most $l-2$. This will follow from Lemma 3.3 without the additional hypothesis (3.4), so we now complete the proof of Lemma 3.3.

5. Completion of the proof of Lemma 3.3. Let f, not a constant, be an element of $\mathfrak{F}_\tau$ maximizing $\mathfrak{L}(f)$ and let $F \in \mathfrak{F}_\tau$, with $F(\lambda_\nu) = 0$ for each λ_ν such that $f(\lambda_\nu) = \pm 1$. Define $g_\epsilon(z) = f(z) + \epsilon F(z)$ with ϵ real. Then $f(z) = \sin \psi(z)$ with $\psi(z)$ defined by (4.4). We can find a point x_1 such that

$$\tfrac{1}{2}\tau \leqq |\psi'(x)| \leqq 2\tau, \qquad |x| \geqq x_1 - 1/(2\tau). \tag{5.1}$$

If $\{\lambda_\nu\}$ are the points where $|f(x)| = 1$, we know that $f'(z)$ has at most $l-1$ zeros besides simple zeros at the λ_ν, so we can choose x_1 also so large that none of these $l-1$ zeros occurs in $|x| \geqq x_1 - 1/(2\tau)$. Finally let x_1 be such that $|f(\pm x_1)| < 1$. In $[-x_1, x_1]$ we have

$$\sup_{-x_1 \leqq x \leqq x_1} |g_\epsilon(x)| = 1 + o(\epsilon), \qquad \epsilon \to 0, \tag{5.2}$$

as was shown in the first part of the proof of Lemma 3.3 in Section 3.

Now consider a point λ_ν in $|x| > x_1$. Since $f(z) = \sin \psi(z)$ where $\psi(z)$ is given by (4.4), and the integrand in (4.4) tends to 1 as $x \to \pm\infty$ through real values, $\psi(x) \sim \tau x$ as $x \to \pm\infty$ and so there are an infinity of λ_ν in $x > x_1$ and in $x < -x_1$. In an interval $|x - \lambda_\nu| < 1/(2\tau)$ we have by (5.1)

$$|x - \lambda_\nu| \, \tau/2 \leqq |\psi(x) - \psi(\lambda_\nu)| \leqq 2\tau \, |x - \lambda_\nu| \leqq 1.$$

Since $\psi(\lambda_\nu) = (n + \frac{1}{2})\pi$ and $\cos\theta \leqq 1 - \theta^2/3$ for $-1 \leqq \theta \leqq 1$ this implies that

$$|f(x)| = |\cos\{\psi(x) - \psi(\lambda_\nu)\}| \leqq 1 - \tau^2 (x - \lambda_\nu)^2/12 \tag{5.3}$$

for $|x - \lambda_\nu| \leqq 1/(2\tau)$. In particular, at the end points of these intervals we have $|f(x)| \leqq \frac{47}{48}$. Now $f'(x)$ has no zeros in the part of $|x| > x_1$ that lies outside these intervals, and so $f(x)$ is montonic in each of them; and there are λ_ν arbitrarily near $\pm\infty$. Hence $|f(x)| \leqq \delta < 1$ in the part of $|x| \geqq x_1$ that lies outside all the intervals, where δ is the maximum of $\frac{47}{48}$, $|f(\pm x_1)|$; so $|g_\epsilon(x)| \leqq 1$ outside these intervals if ϵ is small enough.

Now $|F(x)| \leqq \tau |x - \lambda_\nu|$ since $F(\lambda_\nu) = 0$ and $|F'(x)| \leqq \tau$ by Bernstein's theorem. Hence by (5.3) we have

$$|g_\epsilon(x)| \leqq 1 + 3\epsilon^2, \qquad |x - \lambda_\nu| \leqq 1/(2\tau),$$

if $|\epsilon|$ is sufficiently small. We thus have

$$\sup_{-\infty<x<\infty} |g_\epsilon(x)| = 1 + o(\epsilon), \qquad \epsilon \to 0.$$

This is (3.5), now without any auxiliary hypothesis on $F(z)$, and the proof of Lemma 3.3 can be completed as in Section 3.

6. Completion of the proof of Theorem 1. Now let f be an element of $\mathfrak{F}_\tau$, not a constant, maximizing $\mathcal{L}(f)$. If λ_ν are the distinct real points where $f(x) = \pm 1$ we have shown that $f'(z)$ has at most $l - 1$ zeros besides simple zeros at the λ_ν. We now show that this number is actually at most $l - 2$. If it is $l - 1$, let $p_1(z)$ be a polynomial of degree $l - 1$, with real coefficients, having zeros at the $l - 1$ extra zeros of $f'(z)$, and consider $f'(z)/p_1(z)$. Taking this as the $G(z)$ of Lemma 3.7, we have an element g of $\mathfrak{F}_\tau$ such that $g(\lambda_\nu) = 0$ and $\mathcal{L}(g) \neq 0$. But Lemma 3.3 says that $\mathcal{L}(g) = 0$. This shows that the polynomial $p(z)$ of (2.5) is of degree at most $l - 2$.

We next show that the extremal function in Theorem 1 is unique. Suppose that f_1 and f_2 are two extremal functions, not constants, and consider $f(z) = \frac{1}{2}\{f_1(z) + f_2(z)\}$. Then $f \in \mathfrak{F}_\tau$ and f is also an extremal function. At each real point λ_ν where $f(x) = \pm 1$ we must have $f_1(\lambda_\nu) = f_2(\lambda_\nu) = f(\lambda_\nu) = \pm 1$ since $|f_1(x)| \leqq 1$ and $|f_2(x)| \leqq 1$. Thus $g(z) = f_1(z) - f_2(z)$ has a zero of order at least 2 at each λ_ν. Thus $g(z)$, a function of exponential type τ, has approximately as many zeros as the function $1 - f(z)^2$, which is of order 1 and type 2τ (i.e., not of type less than 2τ), and since most of the zeros of $1 - f(z)^2$ are real, this is impossible. More precisely, f is given by (4.3), where $\psi(x) \sim \tau x$ as $|x| \to \infty$, so the distance between consecutive λ_ν's must be $\pi/\tau + o(1)$ as $|\lambda_\nu| \to \infty$. If $n_\phi(x)$ denotes the number of zeros of the function ϕ in $|z| < x$, we have $n_g(x) \geqq n_h(x)$, $h = 1 - f^2$, and this exceeds $(4\tau/\pi) + o(1)$; while, since g is of the exponential type τ, we have from Carleman's theorem $n_g(x) \leqq (2\tau/\pi)x + o(1)$ (cf. [2], p. 155).

(It would be enough to use the fact ([2], p. 16) that by Jensen's theorem $n_g(x) \leqq \tau x + o(1)$ for an infinity of x tending to ∞.) This contradiction shows that $f_1(z) - f_2(z) \equiv 0$.

Now suppose that $f_1(z) \equiv 1$ and $f_2(z) \not\equiv 1$ are extremal functions. Then $f(z) = \frac{1}{2}\{f_1(z) + f_2(z)\}$ is another non-constant extremal function, which therefore has the form (4.4) and consequently takes negative values; but clearly $f(z) \geqq 0$. This contradiction shows that if an extremal function is constant, there is no other extremal function.

Now we complete the proof of Theorem 1 by showing that the polynomials $p(z)$ and $q(z)$ satisfy

$$q(x) \geqq p(x)^2 \tag{6.1}$$

on the real axis with equalty at some point if and only if p and q are both constant. For, since $f(z)$ belongs to $\mathfrak{F}_\tau$, by a sharpened form of Bernstein's theorem it satisfies ([2], p. 215) $\tau^2 f(x)^2 + f'(x)^2 \leqq \tau^2$, i.e. $\tau^2(1 - f(x)^2) \geqq f'(x)^2$ on the real axis, with equality at some point if and only if $f(x) = \sin(\tau z + \beta)$ for some real β. Combining this with (2.5) we have, at any point where $1 - f^2 \neq 0$, the inequality $p(x)^2/q(x) \leqq 1$, with equality if and only if $f(z) = \sin(\tau z + \beta)$; and in the latter case $p \equiv q \equiv 1$. There remains the possibility that $p(x)^2 = q(x)$ at a point x_1 where $f(x_1) = \pm 1$. In this case the left-hand side of (2.5) approaches $\pm f''(x_1)$ as $x \to x_1$. By Bernstein's theorem, $|f''(x)| < \tau^2$ unless $f(z) \equiv \sin(\tau z + \beta)$, and so again $p(x)^2 < q(x)$ unless $p \equiv q \equiv 1$.

7. Continuity of the extremal function.

We make the following remark, which is useful in analyzing special cases of Theorem 1.

THEOREM 2. *Let $f_\tau(z)$ be the extremal function of Theorem 1. Then $\mathcal{L}(f_\tau)$ and $f_\tau(z)$ are continuous functions of τ in $0 < \tau < \infty$.*

Suppose $\sigma > \tau$. Then $f_\tau(z) \in \mathfrak{F}_\tau \subset \mathfrak{F}_\sigma$, so $\mathcal{L}(f_\tau) < \mathcal{L}(f_\sigma)$. The inequality is strict since f_σ is unique and not of type less than σ. Thus $\mathcal{L}(f_\tau)$ is a strictly increasing function of τ. To show that it is continuous it is then enough to show that

$$\lim_{\sigma \downarrow \tau} \mathcal{L}(f_\sigma) \leqq \mathcal{L}(f_\tau). \tag{7.1}$$

Since $|f_\sigma(x + iy)| \leqq e^{\sigma|y|}$, as $\sigma \to \tau$ through any sequence of values there is a subsequence for which $f_\sigma(z) \to g(z)$, uniformly on compact sets. Then $g(z) \in \mathfrak{F}_\tau$, and since $f_\sigma^{(k)}(x_\nu) \to g^{(k)}(x_\nu)$ it follows that $\mathcal{L}(f_\sigma) \to \mathcal{L}(g) \leqq \mathcal{L}(f_\tau)$. This shows that (7.1) is true.

Now again let $\sigma \to \tau$ through some sequence. Then there is a subsequence such that $f_\sigma(z) \to g(z) \in \mathfrak{F}_\tau$. Since $\mathcal{L}(g) = \lim_{\sigma\to\tau} \mathcal{L}(f_\sigma) = \mathcal{L}(f_\tau)$ and f_τ is unique, $g(z) = f_\tau(z)$.

8. A functional of order 3. The remainder of this paper is principally concerned with finding $A_n(\tau)$ in (1.1) for $n = 1$, when the relevant functional is of order 4. In principle this problem is solved by Theorem 1, but it is not possible to read off numerical results directly from that theorem.

First, however, we shall consider briefly some simpler cases, in particular, functionals of lower order. When $l = 2$, the general functional has the form $\mathcal{L}(f) = \lambda f(a) + \mu f'(a)$. Theorem 1 shows that the unique extremal is either constant or of the form $\sin(\tau z + \sin^{-1} f(0))$. The calculation of the maximum of $\mathcal{L}(f)$ is then elementary.

There are two essentially different types of functionals of order 3, namely

$$\lambda f(0) + \mu f(1) + \gamma f'(1) \tag{8.1}$$

and

$$\lambda f(0) + \mu f'(0) + \gamma f''(0). \tag{8.2}$$

In either case, Theorem 1 shows that the unique extremal is either constant or of the form

$$f(z) = \sin(\tau z + \sin^{-1} f(0)) \tag{8.3}$$

or

$$f(z) = \sin \psi(z), \tag{8.4}$$

$$\psi(z) = \pm \tau \int_0^z \{w - \beta)(w - \bar{\beta})\}^{-\frac{1}{2}} (w - a)\, dw + \sin^{-1} f(0),$$

where a is real and β is not real. Let $b = \Re(\beta)$.

The integral in (8.4) can be evaluated explicitly in terms of elementary functions, and we obtain

$$\begin{aligned}\psi(z) = \pm \tau\{ &\sqrt{(z^2 - 2bz + |\beta|^2)} \\ &+ (b - a)\log(\sqrt{(z^2 - 2bz + |\beta|^2)} + z - b) \\ &- |\beta| - (b - a)\log(|\beta| - b)\} + \sin^{-1} f(0).\end{aligned}$$

If $\sin \psi(z)$ is to be entire, we must have $b - a = 0$ and so

$$\psi(z) = \pm \tau\{\sqrt{(z^2 - 2bz + |\beta|^2)} - |\beta|\} + \sin^{-1} f(0).$$

Thus either

$$\begin{aligned}f(z) = {} &\sin \tau\sqrt{(z^2 - 2bz + |\beta|^2)} \cos(\tau|\beta| - \sin^{-1} f(0)) \\ &- \cos \tau\sqrt{(z^2 - 2bz + |\beta|^2)} \sin(\tau|\beta| - \sin^{-1} f(0))\end{aligned}$$

or

$$f(z) = -\sin\tau\sqrt{(z^2-2bz+|\beta|^2)}\cos(\tau|\beta|+\sin^{-1}f(0)) \\ +\cos\tau\sqrt{(z^2-2bz+|\beta|^2)}\sin(\tau|\beta|+\sin^{-1}f(0)).$$

In either case f can be entire only if the first term on the right vanishes, so that $\tau|\beta|\pm\sin^{-1}f(0)$ must be an odd multiple of $\pi/2$, and then

$$f(z) = \pm\cos\tau\sqrt{(z^2-2bz+|\beta|^2)}. \tag{8.5}$$

We now consider the special case of (8.2) when $\mu=0$, $\gamma>0$. There is then no loss of generality from taking $\gamma=1$, and it is convenient to change the notation and consider

$$\mathscr{L}(f) = \tau^2\lambda f(0)+f''(0). \tag{8.6}$$

Then the maximum of $\mathscr{L}(f)$ is attained either by a constant (± 1); a function of the form $\sin(\tau z+c)$, for which $\mathscr{L}(f)=\tau^2(\lambda-1)\sin c$, whose maximum is $\tau^2|\lambda-1|$; or by a function (8.5).

In the last case put $\beta=re^{i\phi}$. Then

$$\pm\tau^{-2}\mathscr{L}(f) = \lambda\cos\tau r-(\tau r)^{-1}\sin\tau r \\ +((\tau r)^{-1}\sin\tau r-\cos\tau r)\cos^2\phi. \tag{8.7}$$

The maximum modulus of the right-hand side clearly occurs when $\cos^2\phi=0$ or 1. But for the extremal function, β is not real, so we have $\cos\phi=0$. Thus the extremal function is either of the form (8.3) or of the form

$$f(z) = \pm\cos\tau\sqrt{(z^2+r^2)} \tag{8.8}$$

with

$$\pm\tau^{-2}\mathscr{L}(f) = \lambda\cos\tau r-(\tau r)^{-1}\sin\tau r.$$

When $\lambda<0$ the extremal function is given by (8.3). For, the maximum modulus of the right-hand side of (8.7) $(\cos\phi=0)$ is at most $|\lambda|+1$, and this is equal to $|\lambda-1|$ if $\lambda\leqq 0$.

Also, if $f(z)\equiv -1$, $\mathscr{L}(f)=\tau^2|\lambda|<\tau^2|\lambda-1|$.

If f is of the form (8.8), and so $\lambda>0$, then if we set $\theta=\tau r$, we have

$$\mathscr{L}(f) = \tau^2\ \lambda\cos\theta-\theta^{-1}\sin\theta\,| \tag{8.9}$$

for some θ in $0<\theta<\infty$; $\theta=0$ is excluded since $r>0$. In fact, $0<\theta\leqq 2\pi$. For, if $\theta>2\pi$ the uniqueness of the extremal function implies that $|\lambda\cos\theta-\theta^{-1}\sin\theta|$ must be decreased when θ is either increased or decreased by 2π. But this cannot be the case if $\theta>2\pi$.

On the other hand, if $\lambda\geqq\frac{1}{2}$ the extremal function is of the form (8.8).

For, if $\theta = \pi$ then (8.9) shows that $\mathscr{L}(f) \geqq \tau^2\lambda$, and this is at least as large as $\tau^2 \,|\, 1 - \lambda \,|$ when $\lambda \geqq \frac{1}{2}$.

THEOREM 3. *For* $\lambda \leqq \frac{1}{3}$ *the maximum of* $\tau^2\lambda f(0) + f''(0)$ *for* $f \in \mathfrak{F}_\tau$ *is* $\tau^2(1-\lambda)$ *and is attained for the function* $f(z) = -\cos \tau z$. *If* $\lambda > \frac{1}{3}$ *the extremal function f is of the form* $\pm \cos\{\tau(z^2 + r^2)^{\frac{1}{2}}\}$ *and*

$$\mathscr{L}(f) = \tau^2 \max_{0<\theta\leqq\pi} (\theta^{-1}\sin\theta - \lambda\cos\theta). \tag{8.10}$$

If the extremal function is of the form (8.8) then $\lambda > 0$ and $\mathscr{L}(f)$ is given by (8.9) for some θ in $0 < \theta \leqq 2\pi$. If $\pi < \theta \leqq 3\pi/2$, the value of $|\,\lambda\cos\theta - \theta^{-1}\sin\theta\,|$ is increased if we replace θ by $2\pi - \theta$. If $3\pi/2 < \theta \leqq 2\pi$, the value of this same expression is not decreased if we replace θ by $\theta - \pi$. Thus θ lies in $0 < \theta \leqq \pi$, as indicated in (8.10). Now $\mathscr{L}(f) > 0$, so if $\tau^{-2}\mathscr{L}(f) = \lambda\cos\theta - \theta^{-1}\sin\theta$, then $\lambda\cos\theta > \theta^{-1}\sin\theta$ and θ lies in $0 < \theta < \pi/2$. In this case $|\,\lambda\cos\theta - \theta^{-1}\sin\theta\,|$ is not decreased if we replace θ by $\pi - \theta$.

Thus if the extremal function is of the form (8.8) the maximum $\mathscr{L}(f)$ is given by (8.10), with $\lambda > 0$, or is $\tau^2\lambda$, corresponding to $f(z) \equiv 1$. We can exclude the latter possibility, however, since when θ is near π, we have

$$\begin{aligned}\theta^{-1}\sin\theta - \lambda(1-\cos\theta) &= 2\theta^{-1}\sin\tfrac{1}{2}\theta\cos\tfrac{1}{2}\theta - 2\lambda\cos^2\tfrac{1}{2}\theta \\ &= 2\cos\tfrac{1}{2}\theta(\theta^{-1}\sin\theta - \lambda\cos\tfrac{1}{2}\theta) > 0.\end{aligned}$$

The extremal function depends continuously on λ, since it is unique for each λ. If $\lambda \leqq 0$ the extremal function is of the form (8.3) and if $\lambda \leqq \frac{1}{2}$ it is of the form (8.8), so there must be a value of λ for which it changes from one form to the other. The change can occur only when $r = \theta/\tau = 0$. Now

$$\theta^{-1}\sin\theta - \lambda\cos\theta = 1 - \lambda + \theta^2(\tfrac{1}{2}\lambda - \tfrac{1}{6}) + \theta^4(-\tfrac{1}{24}\lambda + \tfrac{1}{120}) - \cdots.$$

Thus $\theta^{-1}\sin\theta - \lambda\cos\theta$ takes values greater than $1 - \lambda$ near $\theta = 0$ if and only if $\lambda > \frac{1}{3}$, so for $\lambda > \frac{1}{3}$ the extremal function is of the form (8.8).

When $\lambda \leqq \frac{1}{3}$ the maximum of $\mathscr{L}(f)$ can also be obtained by using an interpolation series (as in [2], chapter 11):

$$\tau^{-2}\mathscr{L}(f) = (\lambda - \tfrac{1}{3})f(0) = 4\pi^{-2}\sum_{n=1}^{\infty}(-1)^n n^{-2} f(n\pi/\tau).$$

For $\lambda > \frac{1}{3}$ we naturally cannot obtain the best inequality in this way.

9. The maximum of $f'(\frac{1}{2}) - f'(-\frac{1}{2})$.

The functional

$$\mathscr{L}(f) = f'(\tfrac{1}{2}) - f'(-\tfrac{1}{2}),$$

like $f'(\frac{1}{2}) + f'(-\frac{1}{2})$, is of order 4, but it turns out to have a much simpler theory than $f'(\frac{1}{2}) + f'(-\frac{1}{2})$, which we shall consider in Sections 10 ff. If $\mathcal{L}(f)$ attains its maximum for the function $f(z)$ in $\mathfrak{F}_\tau$, it also attains its maximum for the function $f(-z)$, and since the extremal function is unique this shows that f must be even. We showed in Section 6 that $f'(x)$ has at most two zeros ("extra zeros") besides simple zeros at the points where $f(x) = \pm 1$. There are two cases to consider: (i) $|f(0)| < 1$; (ii) $f(0) = \pm 1$. In either case $f'(0) = 0$ since f' is an odd function, and f' has a zero of odd order at 0. In case (i), f' cannot have three or more zeros at 0, so it has just one. If f' has any other extra zeros it has at least two (since it is odd), and so at least three extra zeros in all, which is impossible. Thus in case (i) f' has no extra zeros except at 0, and $p(z) = (z)$ in (4.2).

In case (ii), if f' has any real extra zeros except at 0, it has two between a maximum and a minimum of f and hence (since it is odd, and 0 is an extremum of f) it has four, which is impossible. If the extra zeros are all at 0, there is a triple zero there; in this case, $p(z)^2/q(z)$, when reduced to lowest terms, has only a double zero at 0, so again $p(z) = z$. Thus either $p(z) = z$ or $f'(z)$, if it has extra zeros, has a conjugate imaginary pair which must be pure imaginary, since otherwise since f' is odd) there would be four extra zeros. Thus $f'(\pm ic) = 0$, $c > 0$. Consider the function

$$g(z) = \epsilon f'(z)(z^2 + c^2)^{-1}(z^2 - \tfrac{1}{4}),$$

where ϵ is real. Then $g \in \mathfrak{F}_\tau$ if $|\epsilon|$ is small enough, $g(\lambda) = 0$ for every real zero λ of $1 - f^2$, and (since g is odd) $\mathcal{L}(g) = 2g'(\frac{1}{2}) = 2\epsilon f'(\frac{1}{2})/(\frac{1}{4} + c^2) \neq 0$, since if $f'(\frac{1}{2}) = 0$ and f' is odd, f is certainly not an extremal function. But this contradicts Lemma 10.3. Hence f' has no extra zeros in case (ii).

Thus either $f(z) = \pm \cos \tau z$, corresponding to $p(z) = 1$, or $f(z) = \sin \psi(z)$ with $\psi(z)$ given by (4.4) and $p(w) = w$. In the second case,

$$q(x) = x^2 + ax + b > p(x)^2$$

for all real x, and so $a = 0$ and $b > 0$. Thus if $f(z) \neq \pm \cos \tau z$, we have

$$f(z) = \pm \sin\{\tau \int_0^z (x^2 + c^2)^{-\frac{1}{2}} x\, dx + \lambda\} = \pm \sin\{\tau[(z^2 + c^2)^{\frac{1}{2}} - c] + \lambda\}.$$

Since $f(z)$ is entire, we must then have $\lambda - c\tau = (2k + 1)\pi/2$, and so

$$f(z) = \pm \cos \tau (z^2 + c^2)^{\frac{1}{2}}. \tag{9.1}$$

If $f(z) = \pm \cos \tau z$ we have

$$\mathcal{L}(f) = 2f'(\tfrac{1}{2}) = \pm 2\tau \sin \tfrac{1}{2}\tau.$$

If $f(z)$ is given by (9.1), we have

$$\mathscr{L}(f) = \pm 2\tau\{\sin\tau(\tfrac{1}{4}+c^2)^{\frac12}\}/\{2(\tfrac{1}{4}+c^2)^{\frac12}\}.$$

Hence the maximum of $\mathscr{L}(f)$ is the larger of

$$2\tau\,|\sin\tfrac12\tau\,|, \qquad 2\tau\,|\{\sin\tau(\tfrac14+c^2)^{\frac12}\}/\{2(\tfrac14+c^2)^{\frac12}\}|, \qquad c>0. \tag{9.2}$$

Clearly, if $\tau=2k\pi$ $(k=1,2,\cdots)$ the first expression in (9.2) is zero and the extremal function must be of the form (9.1); while if $\tau=(2k+1)\pi$, the first is 2τ, the maximum permitted by Bernstein's theorem, so the extremal function must be $\pm\cos\tau z$. A complete solution of our problem is given by the following theorem.

THEOREM 4. *Let* t_n $(n=1,2,\cdots)$ *be the root of* $\tan x = x$ *in* $(n\pi,(n+1)\pi)$, *and let* s_n *be the point in* $(n-1)\pi<x<n\pi$ *where* $|\sin s_n|/s_n = |\sin t_n|/t_n$. *Then the function in* $\mathfrak{F}_\tau$ *maximizing* $f'(\frac12)-f(-\frac12)$ *is* $\pm\cos\tau z$ *for* τ *in the intervals* $(0,2s_1),(2t_1,2s_2),\cdots$; *for* τ *in the intervals* $(2s_1,2t_1),(2s_2,2t_2),\cdots$, *it is of the form* (9.1), *and the maximum of* $\mathscr{L}(f)$ *is* $\tau^2|\sin t_n|/t_n$ *if* $2s_n<\tau<2t_n$.

Write $\sigma=\frac12\tau$ and $u^2=1+4c^2>1$. Then the extremal function is of the form (9.1) if and only if the second quantity in (9.2) is larger than the first, i. e.,

$$(\sigma u)^{-2}\sin^2\sigma u > \sigma^{-2}\sin^2\sigma. \tag{9.3}$$

Now the graph of the function $\sigma^{-2}\sin^2\sigma$ consists of a series of arches of decreasing height, with maxima at the points 0, t_n $(n\geqq 1)$. There is a $u>1$ for which (9.3) holds if and only if σ is in the intervals (s_n,t_n) (F. Riesz's "rising sun" lemma), and the largest value of $|\sin u|/(\sigma u)$ is the value of $|\sin\sigma|/\sigma$ at t_n.

10. The maximum of $f'(\frac12)+f'(-\frac12)$. We now consider the case $n=1$ of (1.1). To obtain a symmetric result, let us put $x=-\frac12$ and ask for the maximum of

$$f'(\tfrac12)+f'(-\tfrac12) \tag{10.1}$$

when $f(z)$ is an entire function of exponential type τ with $|f(x)|\leqq 1$ for real x. As we showed in Section 2, there is no loss of generality in taking $f(z)$ real on the real axis, so we may assume that $f\in\mathfrak{F}_\tau$. Then (10.1) is a linear functional of order $l=4$. There is, by Theorem 1, a function f for which (10.1) attains its maximum. Then (10.1) also attains its maximum for the function $-f(-z)$, and since the extremal function is unique this shows that $f(z)$ is an odd function. Hence from Theorem 1 we have

$$f(z) = \sin \psi(z), \tag{10.2}$$

where

$$\psi(z) = \tau\delta \int_0^z \{q(w)\}^{-\frac{1}{2}} p(w)\,dw, \qquad \delta = \pm 1, \tag{10.3}$$

$p(z)$ and $q(z)$ are monic, with real coefficients, and even, with $p(z)$ either constant or of degree 2, and $q(z)$ of twice the degree of $p(z)$ and with no real roots. We take the square root which is positive for real w. For real z we may take the path of integration along the real axis. Then

$$\mathscr{L}(f) = f'(\tfrac{1}{2}) + f'(-\tfrac{1}{2}) = 2\psi'(\tfrac{1}{2}) \cos \psi(\tfrac{1}{2}). \tag{10.4}$$

If $p(w)$ is constant, so is $q(w)$, and then

$$f(z) = \delta \sin \tau z, \qquad \mathscr{L}(f) = 2\delta\tau \cos \tfrac{1}{2}\tau.$$

By Bernstein's theorem we have $|f'(x)| \leqq \tau$ for all real x, so if n is a positive integer and $\tau = 2n\pi$, the function $(-1)^n \sin 2n\pi z$ is the extremal function for (10.1).

If $p(w)$ is not constant, it is of degree 2 and $q(w)$ is of degree 4. We can then write

$$\begin{aligned} p(w)/\{q(w)\}^{\frac{1}{2}} &= (w^2 + \alpha)/\{(w^2 - w_1^2)(w^2 - \bar{w}_1^2)\}^{\frac{1}{2}} \\ &= (w^2 + \alpha)/\{w^4 - 2w^2 r^2 \cos 2\theta + r^4\}^{\frac{1}{2}}, \end{aligned} \tag{10.5}$$

where α is real and $w_1 = re^{i\theta}$, $0 < \theta < \pi/2$.

We first find restrictions imposed on the parameters by the fact that $f(z)$ is entire. Near a zero w_1 of $q(w)$ we see that

$$\psi(z) = \psi(w_1) + (z - w_1)^{\frac{1}{2}} g(z),$$

where $g(z)$ is regular in a neighborhood of w_1. Now

$$\sin \psi(z) = \sin \psi(w_1) \cos \{(z - w_1)^{\frac{1}{2}} g(z)\} + \cos \psi(w_1) \sin \{(z - w_1)^{\frac{1}{2}} g(z)\},$$

so that for $\sin \psi(z)$ to be single-valued we must have $\cos \psi(w_1) = 0$. We can accordingly write

$$\psi(w_1) = \delta(m - \tfrac{1}{2})\pi, \tag{10.6}$$

where m is an integer and δ is the same as in (10.3). (We introduce δ here only to simplify the appearance of later formulas.)

To calculate $\psi(w_1)$ we take as the path of integration the segment of the real axis from $z=0$ to $z=r$ together with the circular arc $w=re^{i\phi}$, $0\leqq\phi\leqq\theta$. Then

$$\psi(w_1)=\tau\delta\int_0^r(x^4-2x^2r^2\cos 2\theta+r^4)^{-\frac{1}{2}}(x^2+\alpha)\,dx$$
$$+\{i\tau\delta/(2r)\}\int_0^\theta(\sin^2\theta-\sin^2\phi)^{-\frac{1}{2}}(r^2e^{2i\phi}+\alpha)\,d\phi.$$

If we put $x=rt$ in the first integral and then take real and imaginary parts (using (10.6)) we find

$$\int_0^\theta(\sin^2\theta-\sin^2\phi)^{-\frac{1}{2}}(\alpha+r^2\cos 2\phi)\,d\phi=0, \tag{10.7}$$

$$(m-\tfrac{1}{2})\pi/(\tau r)=\int_0^1(t^4-2t^2\cos 2\theta+1)^{-\frac{1}{2}}(t^2+\alpha/r^2)\,dt \tag{10.8}$$
$$-\tfrac{1}{2}\int_0^\theta(\sin^2\theta-\sin^2\phi)^{-\frac{1}{2}}\sin 2\phi\,d\phi$$
$$=\int_0^1(t^4-2t^2\cos 2\theta+1)^{-\frac{1}{2}}(t^2+\alpha/r^2)\,dt-\sin\theta.$$

Conversely, if (10.7) and (10.8) are satisfied then if $\psi(z)$ is defined by (10.3), (10.5), the function $f(z)=\sin\psi(z)$ belongs to $\mathfrak{F}_\tau$.

In the next section we shall find a simpler version of the relations among the parameters α, θ, and r implied by (10.5), (10.6). First, however, we shall state our results.

For $n=0,1,2,\cdots$ let χ_n, γ_n be the unique numbers defined by

$$\tfrac{1}{2}\chi_n\tan\tfrac{1}{2}\chi_n=1,\qquad 2n\pi<\chi_n<(2n+1)\pi,$$
$$\gamma_0=\pi,\qquad \tfrac{1}{2}\gamma_n\tan\tfrac{1}{2}\gamma_n=-(\gamma_n{}^2+\pi^2)/(\gamma_n{}^2-\pi^2),$$
$$(2n+1)\pi<\gamma_n<(2n+2)\pi,\qquad\qquad n\geqq 1.$$

We append a short table of χ_n and γ_n, which was computed for us by Marilyn J. Woodyard.

n	0	1	2	3	4	5
$2n\pi$	0	6.28	12.57	18.85	25.13	31.42
χ_n	1.72	6.85	12.87	19.06	25.29	31.54
$(2n+1)\pi$	3.14	9.42	15.71	21.99	28.37	34.56
γ_n	3.14	12.19	18.62	24.97	31.29	37.59

THEOREM 5. *The extremal function* $f(z)$ *in* $\mathfrak{F}_\tau$ *for* $\mathfrak{L}(f)=f'(\tfrac{1}{2})+f'(-\tfrac{1}{2})$ *is* $\sin\tau z$ *in the interval* $0<\tau\leqq\chi_0$; *in the intervals* $\gamma_n\leqq\tau\leqq\chi_{n+1}$,

it is $(-1)^{n+1}\sin\tau z$. *In* $\chi_n < \tau < \gamma_n$, *it is* $\sin\psi(z)$, *where* $\psi(z)$ *is defined by* (10.3), (10.4), *the parameters satisfy* (10.5), (10.6), *with* $m=0$, *and* $\delta=\pm 1$ *is chosen to make* $f'(\tfrac{1}{2})>0$.

More explicitly, the extremal function in $\chi_n < \tau < \gamma_n$ is $\sin\psi(z)$, where

$$\psi(z) = \pm\int_0^{\tau z}\{u^4 - 2u^2\boldsymbol{K}^2\cos 2\theta + \boldsymbol{K}^4\}^{-\frac{1}{2}}\{u^2 + \boldsymbol{K}(\boldsymbol{K} - 2\boldsymbol{E})\}\,du,$$

$\boldsymbol{K}$ and $\boldsymbol{E}$ are complete elliptic integrals of argument $\cos\theta$, and $0<\theta<\pi/2$.

11. Relations among parameters. The integral in (10.7) can be conveniently expressed in terms of complete elliptic integrals. We can write it as

$$\begin{aligned}(1/\sin\theta)\int_0^{\theta}&(1-\csc^2\theta\sin^2\phi)^{-\frac{1}{2}}(\alpha + r^2(1-2\sin^2\phi))\,d\phi\\ &= \csc\theta\{(\alpha + r^2\csc 2\theta)F(\theta,\csc\theta) + 2r^2\sin^2\theta E(\theta,\csc\theta)\}\\ &= (\alpha - r^2)F(\pi/2,\sin\theta) + 2r^2E(\pi/2,\sin\theta)\\ &= (\alpha - r^2)\boldsymbol{K}(\sin\theta) + 2r^2\boldsymbol{E}(\sin\theta),\end{aligned}$$

in the usual notation for elliptic integrals, so that (10.7) states that

$$(11.1)\qquad (\alpha - r^2)\boldsymbol{K}(\sin\theta) + 2r^2\boldsymbol{E}(\sin\theta) = 0.$$

Alternatively, we can calculate $\psi(w_1)$ by taking the path of integration along the imaginary axis from 0 to ir and along the arc $w = re^{i\phi}$, $\pi/2 \geqq \phi \geqq \theta$. Then we obtain

$$\begin{aligned}\psi(w_1) = i\tau\delta\int_0^{r}&\{y^4 + 2y^2r^2\cos 2\theta + r^4\}^{-\frac{1}{2}}(-y^2+\alpha)\,dy\\ &- i\tau\delta/(2r)\int_{\theta}^{\pi/2}(\sin^2\phi - \sin^2\theta)^{-\frac{1}{2}}(r^2e^{2i\phi}+\alpha)\,d\phi.\end{aligned}$$

Taking real parts and using (10.4), we now find

$$\int_{\theta}^{\pi/2}(\sin^2\phi - \sin^2\theta)^{-\frac{1}{2}}(r^2\cos 2\phi + \alpha) = -(2m-1)\pi/(\tau r).$$

This leads to

$$(11.2)\qquad (\alpha + r^2)\boldsymbol{K}(\cos\theta) - 2r^2\boldsymbol{E}(\cos\theta) = -(2m-1)\pi r/\tau.$$

We may abbreviate (11.1), (11.2) in the usual notation as

$$\begin{aligned}&(\alpha - r^2)\boldsymbol{K} + 2r^2\boldsymbol{E} = 0,\\ &(\alpha + r^2)\boldsymbol{K}' - 2r^2\boldsymbol{E}' = pr, \qquad\qquad p = -(2m-1)\pi/\tau.\end{aligned}$$

Solving for α and r, we find, using Legendre's relation $\boldsymbol{E}\boldsymbol{K}' + \boldsymbol{E}'\boldsymbol{K} - \boldsymbol{K}\boldsymbol{K}' = \pi/2$,

$$(11.4) \qquad r = p\boldsymbol{K}/\pi, \qquad \alpha = r^2(\boldsymbol{K} - 2\boldsymbol{E})/\boldsymbol{K} = p^2\boldsymbol{K}(\boldsymbol{K} - 2\boldsymbol{E})/\pi^2.$$

It follows that r and α are continuous functions of θ for $0 < \theta < \pi/2$, since $\boldsymbol{K} > 0$ in this range.

We require a number of lemmas.

LEMMA 11.5. *As* $\theta \to 0$,

$$(11.6) \qquad \alpha/r^2 = -1 + \theta^2 + O(\theta^4),$$

$$(11.7) \qquad (m - \tfrac{1}{2})\pi/(\tau r) = -1 + \tfrac{1}{4}\theta^2 + O(\theta^4).$$

If $\theta \to 0$ *and* $r \geqq \rho > \frac{1}{2}$, *then*

$$(11.8) \qquad p(w)/\{q(w)\}^{\frac{1}{2}} = -1 + \{r^2(r^2 + w^2)/(r^2 - w^2)^2\}\theta^2 + O(\theta^4),$$

uniformly in $0 \leqq w \leqq \frac{1}{2}$.

From (11.4) we have $\alpha/r^2 = (\boldsymbol{K} - 2\boldsymbol{E})/\boldsymbol{K}$, and (11.6) follows from the expansions ([5], p. 3)

$$(11.9) \quad \boldsymbol{K} = \tfrac{1}{2}\pi(1 + \tfrac{1}{4}\sin^2\theta + O(\sin^4\theta)), \quad \boldsymbol{E} = \tfrac{1}{2}\pi(1 - \tfrac{1}{4}\sin^2\theta + O(\sin^4\theta)).$$

We also have $(m - \frac{1}{2})\pi/(\tau r) = -p/(2r) = -\pi/(2\boldsymbol{K})$, and (11.7) follows from (11.9).

To obtain (11.8), write

$$p(w)/\{q(w)\}^{\frac{1}{2}} = \{(w^2 + \alpha)/(r^2 - w^2)\}\{1 + [4r^2w^2/(r^2 - w^2)^2]\sin^2\theta\}^{-\frac{1}{2}}.$$

By (11.6), this is

$$\{-1 + r^2\theta/(r^2 - w^2) + O(\theta^4)\}\{1 - 2r^2w^2\theta^2/(r^2 - w^2)^2 + O(\theta^4)\}$$

and (11.8) follows.

LEMMA 11.10. *As* $\theta \to \pi/2$, *if* $s = \pi/2 - \theta$ *we have*

$$(11.11) \qquad \alpha/r^2 = 1 - 2/\log(4/s) + O(s),$$

$$(11.12) \qquad (m - \tfrac{1}{2})\pi/(\tau r) = -\tfrac{1}{2}\pi/\log(4/s) + O(s),$$

and

$$(11.13) \qquad p(w)/\{q(w)\}^{\frac{1}{2}} = 1 - \{2/\log(4/s)\}\{r^2/(r^2 + w^2)\} + O(s),$$

uniformly in $0 \leqq w \leqq \frac{1}{2}$.

Here we use (11.4) and the expansions ([5], p. 3)

$$\begin{aligned} K &= \log(4/\cos\theta) + \tfrac{1}{4}\{\log(4/\cos\theta) - 1\}\cos^2\theta \\ &\quad + O\{|\log|\cos\theta||\cdot\cos^4\theta\}, \qquad (11.14) \\ E &= 1 + \tfrac{1}{2}\{\log(4/\cos\theta) - \tfrac{1}{2}\}\cos^2\theta + O\{|\log|\cos\theta||\cdot\cos^4\theta\}. \end{aligned}$$

12. Estimates of $\sin\psi(z)$. In this section we consider a function, not necessarily extremal, of the form $f(z) = \sin\psi(z)$, where $\psi(z)$ is defined by (10.3), (10.5), the parameters satisfy (10.7) and (10.8), and δ is the same as in (10.3). We shall obtain several estimates for $f'(\frac{1}{2})$; the error terms are independent of m and τ over any bounded range of τ.

LEMMA 12.1. *If $\theta \to 0$ and $r \geqq \rho > \frac{1}{2}$ then*

$$-\delta f'(\tfrac{1}{2}) = \tau\cos\tfrac{1}{2}\tau + \tau\theta^2\{\tau G(r)\sin\tfrac{1}{2}\tau - H(r,\tfrac{1}{2})\cos\tfrac{1}{2}\tau\} + O(\theta^4),$$

where

$$H(r,w) = r^2(r^2+w^2)/(r^2-w^2)^2, \qquad G(r) = \int_0^{\frac{1}{2}} H(r,w)\,dw.$$

For, by Lemma 11.5,

$$\psi(\tfrac{1}{2}) = \delta\{-\tfrac{1}{2}\tau + \tau G(r)\theta^2 + O(\theta^4\},$$

whence

$$\cos\psi(\tfrac{1}{2}) = \cos\tfrac{1}{2}\tau + \tau G(r)\theta^2\sin\tfrac{1}{2}\tau + O(\theta^4);$$

and

$$\psi'(\tfrac{1}{2}) = \delta\tau\{-1 + H(r,\tfrac{1}{2})\theta^2 + O(\theta^4)\}.$$

Finally $f'(\frac{1}{2}) = \psi'(\frac{1}{2})\cos\psi(\frac{1}{2})$, and the conclusion follows.

LEMMA 12.2. *If $\theta \to \pi/2$ then*

$$\delta f'(\tfrac{1}{2}) = \tau\cos\tfrac{1}{2}\tau + \epsilon\tau(\tfrac{1}{2}\tau\sin\tfrac{1}{2}\tau - \cos\tfrac{1}{2}\tau) + O(\epsilon^2),$$

where

$$\epsilon = 1/\log\{4/(\tfrac{1}{2}\pi - \theta)\}.$$

This follows in the same way from Lemma 11.10.

LEMMA 12.3. *If $\theta \to 0$ and $r \to r_0$, where $0 < r_0 < \frac{1}{2}$, then*

$$\begin{aligned} \delta f'(\tfrac{1}{2}) = \tau\cos\tfrac{1}{2}\tau - \{2\theta^2\tau r_0^2/(1-4r_0^2)\}\{\tau\sin\tfrac{1}{2}\tau \\ + 2(1+4r_0^2)(1-4r_0^2)^{-1}\cos\tfrac{1}{2}\tau\} + O(\theta^2). \end{aligned}$$

For, by Lemma 11.5,

$$\delta\psi(\tfrac{1}{2})/(\tau r) = \int_0^{1/(2r)} \{(t^2-\cos 2\theta)^2 + \sin^2 2\theta\}^{-\frac{1}{2}}(t^2 - 1 + \theta^2 + O(\theta^4))\,dt.$$

We make the substitution $t^2 + \cos 2\theta = u \sin 2\theta$ over the part of the interval of integration where $-\theta^{-\frac{1}{2}} < u < \theta^{-\frac{1}{2}}$, that is, over $t_1 < t < t_2$ where

$$t_1 = \{\cos 2\theta - \theta^{-\frac{1}{2}} \sin 2\theta\}^{\frac{1}{2}} = 1 - \theta^{\frac{1}{2}} - \tfrac{1}{2}\theta - \tfrac{1}{2}\theta^{\frac{3}{2}} - \tfrac{13}{8}\theta^2 + O(\theta^{\frac{5}{2}}),$$

$$t_2 = \{\cos 2\theta + \theta^{-\frac{1}{2}} \sin 2\theta\}^{\frac{1}{2}} = 1 + \theta^{\frac{1}{2}} - \tfrac{1}{2}\theta + \tfrac{1}{2}\theta^{\frac{3}{2}} - \tfrac{13}{8}\theta^2 + O(\theta^{\frac{5}{2}}).$$

The integral defining $\psi(\frac{1}{2})$ will be written as the sum of integrals over the intervals $(0, t_1)$, (t_1, t_2), $(t_2, \frac{1}{2}r^{-1})$.

The integral over (t_1, t_2) is equal to

$$\tfrac{1}{2}\int_{-\theta^{-\frac{1}{2}}}^{\theta^{-\frac{1}{2}}} (u \sin 2\theta - \theta^2 + O(\theta^4))/\{(u^2+1)^{\frac{1}{2}}(\cos\theta + u \sin 2\theta)\}\,du$$

$$= \tfrac{1}{2}(\sec 2\theta)^{\frac{1}{2}} \int_{-\theta^{-\frac{1}{2}}}^{\theta^{-\frac{1}{2}}} \{(u \sin\theta - \theta^2 + O(\theta^4))/(u^2+1)^{\frac{1}{2}}\}$$
$$\times\{1 - \tfrac{1}{2}u \tan 2\theta + \tfrac{3}{8}u^2 \tan^2 2\theta - \tfrac{5}{16}u^3 \tan^3 2\theta$$
$$+ \tfrac{35}{128}u^4 \tan^4 2\theta + O(u^5\theta^5\}\,du.$$

Collecting the even part of the integrand, we see that this integral is equal to

$$-(\sec 2\theta)^{\frac{1}{2}} \int_0^{\theta^{-\frac{1}{2}}} (2u^2\theta^2 + 5u^4\theta^4 + \theta^2)(u^2+1)^{-\frac{3}{2}}\,du + O(\theta^3)$$
$$= -\theta - \tfrac{7}{4}\theta^2 + O(\theta^3).$$

The integral over $(0, t_1)$ is

$$\int_0^{t_1} [\{t^2 - 1 + \theta^2 + O(\theta^4)\}/(1-t^2)]\{1 + 4t^2 \sin^2\theta(1-t^2)^{-2}\}^{-\frac{1}{2}}\,dt$$
$$= \int_0^{t_1} \{-1 + [\theta^2 + O(\theta^4)]/(1-t^2)\}\{1 - 2t^2(1-t^2)^{-2}\sin^2\theta$$
$$+ O(\theta^4/(1-t)^4)\}\,dt$$
$$= \int_0^{t_1} \{-1 + (1+t^2)(1-t^2)^{-2}\theta^2\}\,dt + O(\theta^{\frac{5}{2}})$$
$$= -t_1 + \tfrac{1}{2}\theta^2\{1/(1-t_1) - 1/(1+t_1)\} + O(\theta^{\frac{5}{2}}).$$

The integral over $(t_2, 1/(2r))$ is

$$\int_{t_2}^{1/(2r)} \{(t^2 - 1 + \theta^2 + O(\theta^4))/(t^2-1)\}\{1 + 4t^2(t^2-1)^{-2}\sin^2\theta\}^{-\frac{1}{2}}\,dt$$
$$= \int_{t_2}^{1/(2r)} \{1 - (1+t^2)/(1-t^2)^{-2}\theta^2\}\,dt + O(\theta^{\frac{5}{2}})$$
$$= 1/(2r) - t_2 + \tfrac{1}{2}\theta^2\{1/(1-t_2) + 1/(1+t_2)\} - 2r\theta^2/(4r^2-1)$$
$$+ O(\theta^{\frac{5}{2}}).$$

Adding these results we obtain

$$\delta\psi(\tfrac{1}{2})/(\tau r) = 1/(2r) - 2 + \theta^2\{\tfrac{1}{2} - 2r/(4r^2 - 1)\} + O(\theta^{\frac{5}{2}}).$$

Then, referring to Lemma 11.5, we see that

$$r = r_0(1 + \tfrac{1}{4}\theta^2 + O(\theta^{\frac{5}{2}})), \qquad r_0 = (\tfrac{1}{2} - m)\pi/\tau.$$

Thus

$$\delta\psi(\tfrac{1}{2}) = \tfrac{1}{2}\tau - \theta^2 2\tau r_0/(4r_0^2 - 1) + o(\theta^2),$$

so that

$$\cos\psi(\tfrac{1}{2}) = \cos\tfrac{1}{2}\tau - \theta^2 2\tau r_0(1 - 4r_0^2)^{-1}\sin\tfrac{1}{2}\tau + o(\theta^2).$$

Since the limit of r is less than $\frac{1}{2}$ we have

$$\delta\psi'(\tfrac{1}{2}) = \tau - \theta^2\tau 4r_0^2(1 - 4r_0^2)/(1 - 4r_0^2)^2 + o(\theta^2),$$

and the lemma follows.

13. The case of small τ. We now turn to the proof of the results stated in Theorem 5. In this section we prove that for all small positive τ the extremal function is $f_\tau(z) = \sin\tau z$. We shall sometimes write $\psi_\tau(z)$ instead of $\psi(z)$ since the parameters α, r, θ, δ of the extremal function depend on τ.

Let $0 < \tau < \pi$. As we showed in Section 10, the element of $\mathfrak{F}_\tau$ which maximizes $\mathcal{L}(f)$ is either $f_\tau(z) = \sin\tau z$ or $f_\tau(z) = \sin\psi_\tau(z)$, where $\psi_\tau(z)$ is defined by (10.3), (10.5). The case $f_\tau(z) = -\sin\tau z$ is excluded since $\mathcal{L}(f) > 0$.

The proof that the extremal function is $\sin\tau z$ for all small τ is by contradiction. Suppose that for a sequence of values of τ approaching 0 the extremal function is $f_\tau(z) = \sin\psi_\tau(z)$. Then

$$\psi_\tau'(\tfrac{1}{2})\cos\psi_\tau(\tfrac{1}{2}) > \tau\cos\tfrac{1}{2}\tau.$$

Now $q(w) \geqq p(w)^2$ for real w, so $\cos\psi_\tau(\frac{1}{2}) \to 1$, $\cos\frac{1}{2}\tau \to 1$ as $\tau \to 0$. Also

$$\psi_\tau'(\tfrac{1}{2}) = \tau p_\tau(\tfrac{1}{2})/\{q_\tau(\tfrac{1}{2})\}^{\frac{1}{2}} \leqq \tau,$$

so it follows that

$$p_\tau(\tfrac{1}{2})/\{q_\tau(\tfrac{1}{2})\}^{\frac{1}{2}} \to 1, \qquad \tau \to 0. \tag{13.1}$$

There is a subsequence of values of τ approaching zero such that $\theta \to \theta_0$, $0 \leqq \theta_0 < \pi/2$, and r approaches a limit, finite or infinite. There are several cases to consider.

If $0 < \theta_0 < \pi/2$ then, by (10.7) or (11.4), $\alpha/r^2 \to A$, where $-1 < A < 1$.

But the right-hand side of (10.8) approaches a finite limit as $\theta \to \theta_0$, so (10.8) shows that $r \to \infty$. Then from (10.5) we have

$$|\lim p_\tau(\tfrac{1}{2})/\{q_\tau(\tfrac{1}{2})\}^{\frac{1}{2}}| = |\lim \alpha/r^2| = |A| < 1,$$

and this contradicts (10.1).

If $\theta_0 = 0$, then Lemma 11.5 shows that $r \to \infty$. In Lemma 12.1 we have $\delta = -1$ and

$$f_\tau'(\tfrac{1}{2}) = \tau \cos \tfrac{1}{2}\tau + 2\tau\theta^2 G(r) \cos \tfrac{1}{2}\tau\{\tfrac{1}{2}\tau \tan \tfrac{1}{2}\tau - \tfrac{1}{2}H(r, \tfrac{1}{2})/G(r)\} + o(\theta^2).$$

Now $H(r, w)$ is an increasing function of w in $0 \leqq w \leqq \frac{1}{2}$ so $H(r, \frac{1}{2}) > 2G(r)$. Also $\frac{1}{2}\tau \tan \frac{1}{2}\tau \to 0$ as $\tau \to 0$, so the term in curly brackets is negative. Thus $|f_\tau'(\frac{1}{2})| < \tau |\cos \frac{1}{2}\tau|$ for small τ as $\theta \to 0$.

If $\theta_0 = \pi/2$ then in Lemma 12.2 we have $\delta = 1$ and

$$f_\tau'(\tfrac{1}{2}) = \tau \cos \tfrac{1}{2}\tau + \epsilon\tau \cos \tfrac{1}{2}\tau\{\tfrac{1}{2}\tau \tan \tfrac{1}{2}\tau - 1\} + o(\epsilon).$$

Hence $|f_\tau'(\frac{1}{2})| < \tau |\cos \frac{1}{2}\tau|$ for small τ as $\theta \to \pi/2$.

Thus for all sufficiently small positive τ the extremal function is $\sin \tau z$.

14. Completion of the proof. We know that $f(z) = (-1)^k \sin 2k\pi z$ is the extremal function in $\mathfrak{F}_\tau$ in case $\tau = 2k\pi$. However, in the intervals

$$(14.1) \qquad \chi_n < \tau < \gamma_n, \qquad n = 0, 1, 2, \cdots,$$

the extremal function in $\mathfrak{F}_\tau$ is $\sin \psi(z)$, where $\psi(z)$ is defined by (10.3), (10.5). For, if τ lies in the subinterval $\chi_n < \tau \leqq (2n+1)\pi$ then $\tau |\cos \frac{1}{2}\tau|$ is a decreasing function, and

$$\mathcal{L}(\pm \sin \tau z) = \pm 2\tau \cos \tfrac{1}{2}\tau < (-1)^n 2\chi_n \cos \tfrac{1}{2}\chi_n = \mathcal{L}((-1)^n \sin \chi_n z).$$

Thus for $\chi_n < \tau \leqq (2n+1)\pi$ the extremal function is not $\pm \sin \tau z$ and is therefore $\sin \psi(z)$.

If τ lies in a subinterval $(2n+1)\pi < \tau < \gamma_n$ we shall define a function $f(z)$ belonging to $\mathfrak{F}_\tau$ such that $|f'(\frac{1}{2})| > \tau |\cos \frac{1}{2}\tau|$. For each θ in $0 < \theta < \pi/2$ define α and r by (11.4) with $m = 0$. Thus α and r are functions of θ for each fixed τ, and $r \to r_0 = \pi/(2\tau) < \frac{1}{2}$ as $\theta \to 0$. Substituting these values of α, r, θ with $\delta = \pm 1$ in (10.3), (10.5), we obtain a function $\psi^*(z)$, depending on τ and θ. Then $f^*(z) = \sin \psi^*(z)$ is entire and belongs to $\mathfrak{F}_\tau$. If τ is fixed and $\theta \to 0$, Lemma 12.3 shows that

$$\delta f^{*\prime}(\tfrac{1}{2}) = \tau \cos \tfrac{1}{2}\tau - 4\theta^2 \tau r_0^2 (1 - 4r_0^2)^{-1}$$
$$\times \cos \tfrac{1}{2}\tau\{\tfrac{1}{2}\tau \tan \tfrac{1}{2}\tau + (1 + 4r_0^2)/(1 - 4r_0^2)\} + o(\theta^2).$$

Since τ lies in some interval $(2n+1)\pi < \tau < \gamma_n$ the term in curly brackets is negative. Thus if θ is small, for suitable choice of $\delta = \pm 1$, we have $f^{*\prime}(\frac{1}{2}) > \tau \mid \cos \frac{1}{2}\tau \mid$. The extremal function in $\mathfrak{F}_\tau$ therefore cannot be $\pm \sin \tau z$ and hence must be $\sin \psi(z)$ for some $\psi(z)$ defined by (10.3), (10.5).

Suppose now that for some τ_1 the extremal function is $f_{\tau_1}(z) = \sin \psi_{\tau_1}(z)$. Since $f_\tau(z)$ is a continuous function of τ there is an open interval containing τ_1 for which the extremal function is not $\pm \sin \tau z$ and therefore is $\sin \psi_\tau(z)$. Let (τ', τ'') be the largest such interval containing τ_1. Then

$$(14.2) \qquad f_{\tau'}(z) = \pm \sin \tau' z, \qquad f_{\tau''}(z) = \pm \sin \tau'' z,$$

and $f_\tau(z) = \sin \psi_\tau(z)$ for $\tau' < \tau < \tau''$, where $\psi_\tau(z)$ is given by (10.3) and the parameters satisfy (10.7), (10.8) (or (11.4)). Also $\delta = \pm 1$ is such that $\mathcal{L}(f_\tau) > 0$.

We have to prove that, for some n, $\tau' = \chi_n$, $\tau'' = \gamma_n$.

We note first that because of (14.2) the points τ', τ'' lie outside all the intervals (14.1). Also, since $f_\tau(z)$ depends continuously on τ the parameters θ, α, r are continuous functions of τ for $\tau' < \tau < \tau''$. Thus in (11.8) the integer m must be the same for all τ in $\tau' < \tau < \tau''$.

Now let τ approach one of the endpoints of (τ', τ'') from inside through a sequence of values such that $\theta = \theta(\tau)$ tends to a limit, and $r = r(\tau)$ tends to a limit, finite or infinite. We shall denote this endpoint by τ^*, and write $\theta \to \theta^*$, $0 \leqq \theta^* \leqq \pi/2$.

We show first that $\theta^* = 0$ or $\pi/2$. For, if $0 < \theta^* < \pi/2$ and $r \to \infty$ then (10.7) or (11.4) shows that α/r^2 approaches a limit A, $-1 < A < 1$. Then (10.3), (10.5) show that $f_\tau(z) \to \pm \sin \tau^* A z$, and this contradicts (14.2). If $0 < \theta^* < \pi/2$ and r tends to a finite limit r^* then (11.7) shows that α also tends to a finite limit α^*. Then $\psi_\tau(z)$ tends to a limit defined by (10.3), (10.5) for the parametric values θ^*, r^*, α^* as $\tau \to \tau^*$. This again contradicts (14.2).

If $\theta^* = 0$, then, by Lemma 11.5, the right-hand side of (10.8) approaches -1 and, since m is fixed, this shows that r cannot tend to 0 or ∞. Thus $0 < r^* < \infty$. In case $r^* > \frac{1}{2}$ Lemma 12.1 shows that

$$-\delta f'(\tfrac{1}{2}) = \tau \cos \tfrac{1}{2}\tau + 2\tau\theta^2 G(r) \cos \tfrac{1}{2}\tau \{\tfrac{1}{2}\tau \tan \tfrac{1}{2}\tau - \tfrac{1}{2} H(r, \tfrac{1}{2})/G(r)\} + o(\theta^2).$$

Since τ lies in (τ', τ'') and $f(z)$ is an extremal function we have $\mid f'(\frac{1}{2}) \mid \geqq \mid \cos \frac{1}{2}\tau \mid$. Thus the term in curly brackets is nonnegative, and so is its limit as $\tau \to \tau^*$. Now $H(r^*, w)$ is an increasing function of w in $0 \leqq w \leqq \frac{1}{2}$, so $H(r^*, \frac{1}{2}) > 2G(r^*)$. Thus

$$\tfrac{1}{2}\tau^* \tan \tfrac{1}{2}\tau^* \geqq \tfrac{1}{2}H(r^*, \tfrac{1}{2})/G(r^*) > 1.$$

This shows that τ^* lies in some interval $(\chi_n, (2n+1)\pi] \subset (\chi_n, \gamma_n)$, but this has been excluded.

If $\theta^* = 0$, then $r^* \leqq \frac{1}{2}$, and we now show that $r^* < \frac{1}{2}$. For if $r^* = \frac{1}{2}$, then Lemma 11.5 shows that $(2m-1)\pi/\tau \to -1$ as $\tau \to \tau^*$. But τ^* cannot lie in any interval (14.1), so this is a contradiction.

If $\theta^* = 0$, we show that $\tau^* = \gamma_n$ for some n. For, we have shown that $r^* < \frac{1}{2}$, so Lemma 12.3 applies. Thus

$$\begin{aligned}\delta f'(\tfrac{1}{2}) &= \tau \cos \tfrac{1}{2}\tau - 4\theta^2 \tau r^{*2}(1-4r^{*2})^{-1} \\ &\qquad \times \cos \tfrac{1}{2}\tau\{\tfrac{1}{2}\tau \tan \tfrac{1}{2}\tau + (1+4r^{*2})/(1-4r^{*2})\} + o(\theta^2),\end{aligned}$$

where, by Lemma 11.5,

$$r^* = \lim r = (\tfrac{1}{2} - m)\pi/\tau^*. \tag{14.3}$$

Since τ lies in (τ', τ'') and f is an extremal function we know that $|f'(\frac{1}{2})| > \tau |\cos \frac{1}{2}\tau|$. The term in curly brackets is therefore nonpositive, and so is its limit as $\tau \to \tau^*$. Thus

$$\tfrac{1}{2}\tau^* \tan \tfrac{1}{2}\tau^* \leqq -(1+4r^{*2})/(1-4r^{*2}). \tag{14.4}$$

We recall that $0 < r^* < \frac{1}{2}$. Then in (14.3), m is 0 or a negative integer. The point τ^* cannot lie in any interval (14.1), and this shows both that (14.4) is an equality and that $m = 0$ in (14.3). Thus $\tau^* = \gamma_n$ for some n. Now m in (14.3) is the same integer m that occurs in (10.8) for all τ in the interval $\tau' < \tau < \tau''$. Thus if $\theta^* = 0$ then for all τ in $\tau' < \tau < \tau''$ the parameters of the extremal function satisfy (10.8) with $m = 0$.

If $\theta^* = \pi/2$ then Lemma 12.2 shows that

$$\delta f'(\tfrac{1}{2}) = \tau \cos \tfrac{1}{2}\tau + \epsilon\tau \cos \tfrac{1}{2}\tau\{\tfrac{1}{2}\tau \tan \tfrac{1}{2}\tau - 1\} + o(\epsilon).$$

Since f is an extremal function we have $|f'(\frac{1}{2})| > \tau |\cos \frac{1}{2}\tau|$, and since $\tau \to \tau^*$ this implies that $\frac{1}{2}\tau^* \tan \frac{1}{2}\tau^* \geqq 1$. If this were a strict inequality, τ^* would lie in one of the intervals (14.1), and this is impossible. Thus $\tau^* = \chi_n$ for some n.

We have thus shown that the open interval (τ', τ'') has its end points in the sets $\{\chi_n\}$, $\{\gamma_n\}$. On the other hand, the interval cannot contain any point $2k\pi$ since at these points the extremal function in $\pm \sin 2k\pi z$. It follows that for some nonnegative n we have $\tau' = \chi_n$, $\tau'' = \gamma_n$. Then $\theta \to \pi/2$ as $\tau \to \tau' = \chi_n$ and $\theta \to 0$ as $\tau \to \tau'' = \gamma_n$ through values in (τ', τ'').

As τ moves from τ' to τ'' the angle θ moves from $\pi/2$ to 0, taking all values in $(0, \pi/2)$. The parameters satisfy (10.7), (10.8), or (11.3), (11.4), with $m = 0$. The left-hand side of (10.8) is never zero for $\tau' < \tau < \tau''$, so the right-hand side of (10.8) is never zero for $0 < \theta < \pi/2$ when the value of α/r^2 in (10.8) is that determined by (10.7).

In the intervals in which the extremal function has the form $\sin \psi(z)$, the maximum of $\mathcal{L}(f)$ could be calculated for any given τ by determining α and r from (11.3), (11.4) and calculating the maximum of $\mathcal{L}(f)$ as a function of θ.

15. Functionals which involve no derivatives. If all $n_\nu = 0$ in (2.1), i.e., if $\mathcal{L}(f)$ has the form

$$\mathcal{L}(f) = \sum_{\nu=1}^{m} \alpha_\nu f(x_\nu), \tag{15.1}$$

Theorem 1 does not apply. For example, if

$$\mathcal{L}(f) = f(\tfrac{1}{2}) - f(-\tfrac{1}{2}), \tag{15.2}$$

then when $\tau > \pi$, an obvious extremal function is $f(z) = \sin \pi z$, which is of type less than τ; and if $\tau > 3\pi$ another extremal function is $f(z) = -\sin \frac{3}{2}\pi z$, so that the extremal function is not unique. However, functionals (15.1) can be discussed by using the following device. Consider the functional

$$\mathcal{L}_t(f) = tf'(x_1) + \mathcal{L}(f), \qquad t > 0. \tag{15.3}$$

This is a functional of order $m + 1$ to which our theory applies for each t. Let $f_t(z)$ be the extremal function for $\mathcal{L}_t$. Then $\{f_t(z)\}$, where t runs through a sequence whose limit is 0, is a normal family; let $f_0(z)$ be a limit function of this family. Then f_0 is an extremal function for the functional $\mathcal{L}$. For, by Bernstein's theorem,

$$\mathcal{L}(f_t) = \mathcal{L}_t(f_t) - tf_t'(x_1) \geqq \mathcal{L}_t(f_t) - t\tau.$$

We know from Lemma 2.2 that there is at least one extremal function f_1 for $\mathcal{L}$. Then

$$tf_t'(x_1) + \mathcal{L}(f_t) = \mathcal{L}_t(f_t) \geqq \mathcal{L}_t(f_1) = tf_1'(x_1) + \mathcal{L}(f_1).$$

Since $f_t'(x_1) \to f_0'(x_1)$ and $\mathcal{L}(f_t) \to \mathcal{L}(f_0)$, it follows that $\mathcal{L}(f_0) \geqq \mathcal{L}(f_1)$.

Since f_1 is extremal for $\mathcal{L}$, so is f_0, and $\mathcal{L}(f_0)=\mathcal{L}(f_1)$. Now since f_t is of order $m+1$, either f_t is a constant or

$$f_t(z)=\sin\psi_t(z), \tag{15.4}$$

where

$$\psi_t(z)=\pm\tau\int_0^z\{q_t(w)\}^{-\frac{1}{2}}p_t(w)\,dw+\sin^{-1}f_t(0), \tag{15.5}$$

p_t is of degree at most $m-1$ and q_t is of degree twice that of p_t, and the other conclusions of Theorem 1 hold.

As $t\rightarrow 0$ either the coefficients of p_t and q_t are bounded and we can select a sequence of t's so that p_t and q_t approach limits of the same kind; or the coefficients of p_t and q_t are unbounded, in which case the integrand of $\psi_t(z)$ approaches a function of the same form, $p(w)/\{q(w)\}^{\frac{1}{2}}$, but with p and q not necessarily monic. Hence we can obtain an extremal function for $\mathcal{L}$ by taking either a constant, or a function of the form described in Theorem 1, or one of the same form with p of degree at most $l-2$, but with τ possibly replaced by a smaller number.

The simplest nontrivial functional of the kind under consideration is $\mathcal{L}(f)=f(\frac{1}{2})-f(-\frac{1}{2})$, which was considered by S. Bernstein [1]. He showed that an extremal function is $\sin\tau z$ if $0<\tau\leqq\pi$, when $\max\mathcal{L}(f)=2\sin\frac{1}{2}\tau$ (see also [2], p. 214); while if $\tau>\pi$ an extremal function is $\sin\pi z$ and $\max\mathcal{L}(f)=2$. Here, although the variational method can be used, it is not advantageous since the extremal functions can be completely determined by more direct methods. The same is true for

$$\mathcal{L}(f)=f(-1)-2f(0)+f(1).$$

However, the less symmetrical functional

$$\mathcal{L}(f)=f(-1)+f(0)-f(1)$$

is better suited to our method. For possible extremal functions of the form $\sin(\sigma z+c)$ we have $\max\mathcal{L}(f)=(1+4\sin^2\sigma)^{\frac{1}{2}}$, which is actually extremal for sufficiently small σ. On the other hand, our method also suggests possible extremal functions of the form

$$f(z)=\pm\cos\sigma\sqrt{(z^2+2rz\cos\phi+r^2)}, \tag{15.6}$$

and for sufficiently large σ we can make $\mathcal{L}(f)$ for such a function attain the largest possible value, namely 3. Hence there is a number σ such that (15.6) is an extremal function for $\mathcal{L}$ in $\mathfrak{F}_\tau$ for all $\tau\geqq\sigma$. It is possible that functions of the kind considered in Theorem 5 are extremal for an intermediate range of values of τ, but we have not investigated this possibility.

NORTHWESTERN UNIVERSITY,
UNIVERSITY OF WISCONSIN.

REFERENCES.

[1] S. Bernstein, "Extension of an inequality of S. B. Stechkin to entire functions of finite degree," *Doklady Akademiya Nauk SSSR*, vol. 60 (1948), pp. 1487-1490 = Sobranie Sochinanii, vol. 2, 1954, Akademiya Nauk SSSR, pp. 442-445.

[2] R. P. Boas, Jr., *Entire functions*, Academic Press, New York, 1954.

[3] ———, and A. C. Schaeffer, "New inequalities for entire functions," to appear in *Journal of Mathematics and Mechanics.*

[4] P. L. Chebyshev, "Théorie des mécanismes connus sous le nom de parallélogrammes," *Mémoires de l'Académie de Sciences de St. Pétersbourg*, vol. 7 (1854), pp. 539-568 = Polnoe Sobranie Sochinenii, vol. 2, Moscow-Leningrad, 1947, pp. 23-51.

[5] F. Oberhettinger and W. Magnus, *Anwendung der elliptischen Funktionen in Physik und Technik*, Springer, Berlin-Göttingen-Heidelberg, 1949.

[6] G. Zolotareff, "Sur l'application des fonctions elliptiques aux questions de maxima et minima," *Bulletin de l'Académie des Sciences de St.-Pétersbourg* (3), vol. 24 (1878), pp. 305-310; *Oeuvres*, vol. 1, pp. 369-374; vol. 2, pp. 130-166.

ON KAEHLERIAN HOMOGENEOUS SPACES OF UNIMODULAR LIE GROUPS.*

By JUN-ICHI HANO.

Recently the results of E. Cartan on Hermitian symmetric space have been extended to the case of Kaehlerian homogeneous spaces by several authors. In particular the structure of compact Kaehlerian homogeneous spaces has been fully exploited. As for the non-compact case, there are few known results except in the case where the groups are semi-simple or reductive. A. Borel [1] and J. L. Koszul [6] have studied the structure of Kaehlerian homogeneous spaces of semi-simple Lie groups and have shown, independently of each other, an interesting result that a bounded domain in a unitary space admitting a transitive semi-simple Lie group of complex analytic homeomorphisms is symmetric. This result gives a partial answer to the problem of E. Cartan. In his important paper in 1935 [2], E. Cartan raised the question whether a bounded homogeneous domain is always a symmetric bounded domain. Y. Matsushima [8] has studied the structure of Kaehlerian homogeneous spaces of reductive Lie groups and has shown that these spaces are the direct product of a locally flat Kaehlerian space and a Kaehlerian homogeneous space of a semi-simple Lie group.

The purpose of the present paper is to study the structure of Kaehlerian homogeneous spaces of a more general class of Lie groups, that is, those of unimodular Lie groups. Specifically, we shall deal with the following two cases. First we shall consider the case where the isotropy group is semi-simple and obtain the following two theorems:

THEOREM I. *If a homogeneous space of a connected unimodular Lie group by a closed connected semi-simple subgroup admits an invariant Kaehlerian structure, then the Kaehlerian structure is locally flat.*

THEOREM II. *If a connected unimodular Lie group has a left invariant Kaehlerian structure, then the group is meta-abelian. Especially if the group is nilpotent, then it must be abelian.*[1]

---

* Received April 15, 1957; revised September 18, 1957.

[1] The last part of Theorem 2 is a generalization of a result of Koszul (unpub-

Secondly we deal with a Kaehlerian homogeneous space of a unimodular Lie group whose Ricci curvature is non-degenerate and prove the following:

THEOREM III. *If the Ricci curvature of a Kaehlerian homogeneous space of a connected unimodular Lie group is non-degenerate and if the group acts effectively on the space, then the group is semi-simple.*

A bounded domain in a unitary space has the Bergman metric which is Kaehlerian and invariant by all complex analytic homeomorphisms of the domain. If a bounded domain admits a transitive group of complex analytic homeomorphisms, the Ricci curvature of the Bergman metric coincides with the metric itself, and hence it is positive definite. Therefore, from Theorem III and from the result of A. Borel and J. L. Koszul mentioned above, we have the following answer to the problem of E. Cartan:

THEOREM IV. *A bounded domain which admits a transitive connected unimodular Lie group of complex analytic homeomorphisms is symmetric.*

We remark that these theorems hold true under a slightly weaker assumption which is explained in **4**, and that in order to prove Theorem III, we only use the result in **6** concerning the Ricci curvature of a Kaehlerian homogeneous space.

The author wishes to express here his sincere thanks to Professor Y. Matsushima and Professor K. Nomizu for their kind suggestions and valuable criticism during the preparation of this paper.

I. Preliminaries.

1. Let G be a connected Lie group and let B be a closed subgroup of G. We denote by $\mathfrak{g}$ the Lie algebra of all left invariant vector fields on G and by $\mathfrak{b}$ the subalgebra of $\mathfrak{g}$ consisting of all left invariant vector fields which are tangent to B at the identity e. Let G/B be the homogeneous space of left cosets of G by B, and let π be the projection from G onto G/B. The differential π_e of π at the identity e maps the tangent space $\mathfrak{g}_e$ of G at e onto the tangent space T_o of G/B at o, where o denote the point $\pi(e)$. By assigning $\pi_e(X_e)$ to each $X \in \mathfrak{g}$, we have the linear mapping π' from $\mathfrak{g}$ onto T_o, where X_e is the value at e of the vector field X.

When $\mathfrak{g}$ has a direct sum decomposition $\mathfrak{g} = \mathfrak{b} + \mathfrak{m}$ into two subspaces

---

lished). He has proved the same result for rational nilpotent Lie groups. He has also proved that if a compact homogeneous space of a nilpotent Lie group admits a Kaehlerian structure, not necessarily invariant, the group must be abelian.

$\mathfrak{b}$ and $\mathfrak{m}$ such that $\mathrm{ad}\, b \cdot \mathfrak{m} \subset \mathfrak{m}$ for all $b \in B$, the homogeneous space G/B is called a reductive homogenous space by Nomizu [10]. We shall call this decomposition of $\mathfrak{g}$ an $\mathrm{ad}\, B$-stable decomposition. When, more strongly, the induced representation of B on the Grassmann algebra of $\mathfrak{g}$ is completely reducible, we say that the subgroup B is reductive in G according to Koszul [5]. Clearly, if B is reductive in G, G/B is a reductive homogeneous space.

A homogeneous space G/B having a Riemannian metric invariant by the group G is called a Riemannian homogeneous space. We shall prepare the following proposition for later use.

(1.1) *Let G/B be a Riemannian homogeneous space. If G operates effectively on G/B, then the subgroup B is reductive in G.*

In fact, let us consider the largest connected group G^* of isometries. It is known that G^* is a Lie group and the isotropy subgroup B^* at o is compact. Hence the Lie algebra $\mathfrak{g}^*$ of G^* has a positive definite symmetric bilinear form f^* invariant by $\mathrm{ad}\, b$ for all $b \in B^*$. Since G is effective on G/B, G can be embedded in G^* as a Lie subgroup. The restriction f of f^* on the subalgebra $\mathfrak{g}$ is evidently a positive definite symmetric bilinear form and invariant by $\mathrm{ad}\, b$ for all $b \in B$. The Grassmann algebra of $\mathfrak{g}$ has a positive definite symmetric bilinear form induced by f, which is invariant by the induced representation of B on the Grassmann algebra. Therefore this representation is completely reducible, and our assertion is proved.

2. Let G/B be a reductive homogeneous space and let $\mathfrak{g} = \mathfrak{b} + \mathfrak{m}$ be an $\mathrm{ad}\, B$-table decomposition. The subscript $\mathfrak{m}$ (resp. $\mathfrak{b}$) of an element X in $\mathfrak{g}$ means the $\mathfrak{m}$-component (resp. the $\mathfrak{b}$-component) of X with respect to this decomposition. The restriction of π' on $\mathfrak{m}$ gives an isomorphism from $\mathfrak{m}$ onto T. Hereafter, when we consider a reductive homogeneous space, we shall identify the tangent space T_o of G/B at o with the subspace $\mathfrak{m}$ by this isomorphism.

Now, we assume that G/B has an invariant Riemannian metric g. Following Nomizu [9], we shall prepare some fundamental notions of an invariant Riemannian connection on G/B. Let X be an element in $\mathfrak{m}$. We denote by σ_t the one-parameter subgroup generated by $X \in \mathfrak{m}$. We set $\sigma_t \cdot o = \tau_t$. Clearly σ_t defines the type preserving isomorphism from the tensor algebra at o onto the tensor algebra at τ_t, which we denote also by σ_t. Moreover, we denote by ρ_t^{-1} the parallel translation from τ_t to o along the curve τ_t in the opposite direction, which is defined by the Riemannian connection associated to the metric g. We have the linear mapping D_X of the tensor algebra of $\mathfrak{m}$ defined by

$$D_X A = \lim_{t\to 0}(\rho_t^{-1}\cdot\sigma_t A - A)/t, \text{ where } t\to 0,$$

for all tensors A on $\mathfrak{m}$. Clearly D_X preserves the type of tensors and is linear with respect to X. Moreover, D_X satisfies the following conditions:

(2.1) $\operatorname{ad} b\cdot D_X Y = D_{\operatorname{ad} b\cdot X}\operatorname{ad} b\cdot Y$ for all $X, Y\in\mathfrak{m}$ and for all $b\in B$.

(2.2) $g(D_X Y, Z) + g(Y, D_X Z) = 0$ for all $X, Y, Z\in\mathfrak{m}$.

(2.3) $D_X Y - D_Y X - [X, Y]_{\mathfrak{m}} = 0$ for all $X, Y\in\mathfrak{m}$.

(2.4) If a tensor field a on G/B is G-invariant, $D_X a$ coincides with the covariant derivative of a at o along X.

The value at o of the curvature tensor field R, of type (1.3), is given by

$$R_o(X, Y)Z = [D_X, D_Y]Z - D_{[X,Y]_{\mathfrak{m}}}Z - \operatorname{ad}[X, Y]_{\mathfrak{b}}Z$$

for all $X, Y, Z\in\mathfrak{m}$. The value at o of the Ricci curvature r is given by $r_o(X, Y) = \operatorname{tr}_{\mathfrak{m}}(Z\to R_o(Y, Z)X)$ for all $X, Y\in\mathfrak{m}$.

Let G/B be a simply connected Riemannian homogeneous space. Since a Riemannian homogeneous space is complete, G/B has the canonical decomposition with respect to the homogeneous holonomy group given by de Rahm [3]. G/B is a Riemannian direct product of spaces $M_o, M_1, \cdots, M_s$, where M_o is a Euclidean space and M_i, $1\leqq i\leqq s$, has the non-trivial irreducible homogeneous holonomy group. Moreover each M_i is isometric to the Riemannian homogeneous space G_i/B of a connected closed subgroup G_i in G containing the subgroup B ([10], Theorem 3). We can denote this decomposition by $G_o/B\times G_1/B\times\cdots\times G_s/B$.

Now let I be a G-invariant tensor field of type (1,1) defining an invariant complex structure on a homogeneous space G/B. By a result of Koszul [6], the value I_o at o of I satisfies the following conditions:

$$(\operatorname{ad} b)_{\mathfrak{m}}\cdot I_o = I_o\cdot(\operatorname{ad} b)_{\mathfrak{m}} \text{ for all } b\in \mathrm{B},$$

$$I_o[X, Y]_{\mathfrak{m}} - [I_o X, Y]_{\mathfrak{m}} - [X, I_o Y]_{\mathfrak{m}} - I_o[I_o X, I_o Y]_{\mathfrak{m}} = 0 \quad \text{for all } X, Y\in\mathfrak{m}.$$

When G/B has an invariant complex structure, an invariant Riemannian metric g on G/B is called Hermitian if g satisfies the condition: $g(IX, IY) = g(X, Y)$ for any vector fields X, Y on G/B. In this case we have a 2-form Ω given by $\Omega(X, Y) = g(IX, Y)$ for all vector field X, Y on G/B, which is called the Kaehlerian form associated to the Hermitian metric g. Of course, Ω is G-invariant. If the Kaehlerian form Ω is a cocycle, that is,

$d\Omega = 0$ we call the pair of the complex structure I and the Hermitian metric g an invariant Kaehlerian structure. A homogeneous space having an invariant Kaehlerian structure is called a Kaehlerian homogeneous space. It is well known that a G-invariant Hermitian metric g on a complex homogeneous space G/B, defines a Kaehlerian structure if and only if the covariant differential of the tensor field I is equal to zero. When G/B is a reductive homogeneous space, this condition is equivalent to the following:

$$(2.5) \qquad D_X \cdot I_o = I_o \cdot D_X \quad \text{for all } X \in \mathfrak{m}.$$

The value at o of the Ricci curvature r associated to an invariant Kaehlerian structure may be expressed by

$$r_o(X, Y) = \tfrac{1}{2}\mathrm{tr}_{\mathfrak{m}} I_o \cdot R(I_o X, Y),$$

a formula which is equivalent to the one in [7]. The bilinear form defined by $\alpha(X, Y) = r(IX, Y)$ for all vector fields X, Y is a G-invariant exterior form of degree two. We call this 2-form α the Ricci form.

3. Let $C^*(G)$ be the Grassmann algebra of all left invariant differential forms on a connected Lie group G. Let $C^p(G)$ be the subspace of $C^*(G)$ consisting of all homogeneous elements of degree p. We denote by w the linear mapping of $C^*(G)$ such that $wa = (-1)^p a$ for all $a \in C^p(G)$. For each $a \in C^*(G)$, we have the linear mapping $\epsilon(a)$ of $C^*(G)$ given by $\epsilon(a)b = a \wedge b$ for all $b \in C^*(G)$. For each $X \in \mathfrak{g}$, we have the linear mapping $\iota(X)$ of $C^*(G)$ such that 1) $\iota(X)a = 0$ for all $a \in C^\circ(G)$ 2) if $a \in C^p(G)$ $(p \geqq 1)$,

$$(\iota(X)a)(X_1, \cdots, X_{p-1}) = \frac{1}{p} a(X, X_1, \cdots, X_{p-1})$$

for all $X_1, \cdots, X_{p-1} \in \mathfrak{g}$. We know that $\iota(X)$ is an anti-derivation of $C^*(G)$, i.e. $\iota(X)(a \wedge b) = \iota(X)a \wedge b + wa \wedge \iota(X)b$ for all $a, b \in C^*(G)$. Moreover, for each $X \in \mathfrak{g}$, the derivation $\theta(X)$ of $C^*(G)$ is defined by

$$(\theta(X)a)(X_1, \cdots, X_p) = -\sum_{1 \leqq i \leqq p} a(X_1, \cdots, [XX_i], \cdots, X_p)$$

for all $a \in C^p(G)$ and for all $X_1, \cdots, X_p \in \mathfrak{g}$; $\theta(X)$ is nothing but an infinitesimal transformation defined by the right invariant vector field X' whose value at e coincides with X_e. If $a \in C^*(G)$, the exterior differential da is also contained in $C^*(G)$. The following relation among these operations will be used frequently:

$$(3.1) \qquad \theta(X) = \iota(X)d + d\iota(X).$$

We denote by $H^*(G)$ the cohomology algebra of $C^*(G)$ with respect to the coboundary operator d.

Let G/B be a homogeneous space of a connected Lie group G. We denote by $C^*(G/B)$ the space of all G-invariant differential forms on G/B. Clearly $C^*(G/B)$ is finite dimensional over the field of all real numbers. We denote $C^p(G/B)$ the subspace of all homogeneous elements of degree p. Since the exterior differential da of $a \in C^*(G/B)$ also belongs to $C^*(G/B)$, we have the cohomology algebra $H^*(G/B)$ of $C^*(G/B)$ with respect to d. Let π^* be the dual of the differential of the projection π from G onto G/B, and let $L^*(G/B)$ be the image of $C^*(G/B)$ by π^*. Obviously $L^*(G/B)$ is a subalgebra of $C^*(G)$ and is equal to the subspace of all element $a \in C^*(G)$ such that 1) $\iota(X)a = 0$ for all $X \in \mathfrak{b}$ and 2) the right translation defined by any $b \in B$ leaves a variant. Since the exterior differentiation and π^* are commutative, $L^*(G/B)$ is d-stable.

We denote by $N^1(G:B)$ the subspace of $C^1(G)$ consisting of all elements a such that $\iota(X)a = 0$ for all $X \in \mathfrak{b}$, and by $N^*(G:B)$ the subalgebra in $C^*(G)$ generated by 1 and $N^1(G:\mathrm{B})$. The subalgebra $N^*(G:B)$ is the direct sum of its homogeneous parts $N^p(G:B) = N^*(G:B) \cap C^p(G)$, and is $\mathfrak{b}$-stable, i.e. $\theta(X)$ leaves $N^*(G:B)$ stable for all $X \in \mathfrak{b}$. We say that an element $a \in C^*(G)$ is $\mathfrak{b}$-invariant if $\theta(X)a = 0$ for all $X \in \mathfrak{b}$. We denote by $L^*(G:B)$ the subalgebra of all $\mathfrak{b}$-invariant elements in $N^*(G:B)$; $L^*(G:B)$ is the direct sum of its homogeneous parts $L^p(G:B) = L^*(G:B) \cap C^p(G)$. In virtue of (3.1), the exterior differentiation d leaves $L^*(G:B)$ stable. We can easily see that the subalgebra $L^*(G/B)$ is contained in $L^*(G:B)$ and that if B is connected, $L^*(G:B)$ coincides with $L^*(G/B)$.

For an arbitrary differential form a on a manifold, we have also the operation $\epsilon(a)$ which maps any differential form b to $a \wedge b$. When a manifold has a Riemannian metric g, we have the dual operation $\iota(a)$ of $\epsilon(a)$ given by $g(\iota(a)b, c) = g(b, \epsilon(a)c)$ for all differentials forms b and c.

4. Later on we shall have frequently to do with the condition that the highest dimensional homogeneous part of $H^*(G/B)$ does not vanish, which we now explain. This condition is equivalent to the following two conditions: 1) there exists a G-invariant n-form, where $n = \dim G/B$, and 2) $dC^{n-1}(G/B) = 0$. By a theorem given by Koszul ([5], Theorem 12.1), we know that if a connected Lie group G is unimodular and if a closed connected subgroup B is reductive in G, then $\dim H^n(G/B) = 1$. We prove the following proposition:

(4.1) *If a Riemannian homogeneous space of a connected unimodular Lie group G is orientable and if G acts effectively on G/B, then* $\dim H^n(G/B) = 1$.

In fact, since G/B is orientable, there exists a G-invariant non-zero n-form, the so-called volume element. Since G is effective on G/B, we have, as is already seen in **1**, a positive definite symmetric bilinear form on the Lie algebra $\mathfrak{g}$, which is $\operatorname{ad} b$-invariant for all $b \in B$. Hence, the connected component $B_\circ$ of B is also reductive in G. Applying the above theorem of Koszul for the pair of G and $B_\circ$, we have $dC^{n-1}(G/B_\circ) = 0$ and hence $dL^{n-1}(G/B_\circ) = 0$. Since $B_\circ$ is connected, we have $dL^{n-1}(G:B_\circ) = 0$. Clearly $L^{n-1}(G/B)$ is contained in $L^{n-1}(G:B_\circ)$, and hence we have $dL^{n-1}(G/B) = 0$, which implies $dC^{n-1}(G/B) = 0$. Thus our assertion is proved.

Conversely, if $\dim H^n(G/B) = 1$, the space G/B is orientable.

II. Invariant forms on a Riemannian homogeneous space.

5. Let us consider an orientable n-dimensional Riemannian homogeneous space G/B with metric tensor field g. Since G/B is orientable, there exists a differential form v of degree n which is invariant by G and has the unit length. Making use of v, the star operator $*$ is defined by $*a = \iota(a)v$ for any differential form a on G/B. We define the codifferential operator δ by $\bar{w} * d * w$, where w (resp. $\bar{w}$) is the linear mapping such that $wa = (-1))^p a$ (resp. $\bar{w}a = (-1)^{p(n+1)}a$) for any p-form a. The Laplacian operator Δ is given by $\delta d + d\delta$, and we say that a differential form a is harmonic if and only if $\Delta a = 0$. Since these operators commute with the transformations in G, they leave $C^*(G/B)$ stable.

We shall give expressions of the operators d, δ and Δ in terms of covariant differentiation. For this purpose, let us take a frame $\{X_1, \cdots, X_n\}$ on an open set and let $\{\omega^1, \cdots, \omega^n\}$ be the dual frame of $\{X_1, \cdots, X_n\}$. Then we have

$$d = \sum_{1 \leqq i \leqq n} \epsilon(\omega^i) \nabla_{X_i}, \qquad \delta = -\sum_{1 \leqq i \leqq n} \iota(\omega^i) \nabla_{X_i},$$

where ∇_X denotes the covariant differentiation along the vector field X. If a is a 1-form, we have

$$\Delta a = -\sum_{1 \leqq i \leqq n} (\nabla_{X_i} \nabla_{X_i} - \nabla_{\nabla_{X_i} X_i}) a - \sum_{1 \leqq i, j \leqq n} \epsilon(\omega^i) \iota(\omega^j) R(X_i, X_j) a.$$

When a is a G-invariant 1-form, $g(a, a)$ is a constant over GB, and hence we have $g(\nabla_X a, a) = 0$. It follows that if $a \in C^1(G/B)$, then

$$g(\Delta a, a) = \sum_{1 \leqq i \leqq n} g(\nabla_{X_i} a, \nabla_{X_i} a) - r(a, a),$$

where r is the bilinear form on $C^1(G/B)$ given by the Ricci curvature r. On account of this formula, we obtain the following proposition:

(5.1) *Let G/B be an orientable Riemannian homogeneous space. If a G-invariant 1-form a on G/B is harmonic and if $r(a, a) = 0$, then a is a parallel field.*

Now, we restrict our consideration to $C^*(G/B)$. For any two elements $a, b \in C^*(G/B)$, $g(a, b)$ is a constant over G/B. We can regard g as an inner product on the finite dimensional vector space $C^*(G/B)$ over the field of all real numbers. Using a property of the star operator, we have

$$*d(a_\wedge * b) = *(da_\wedge * b) + *(wa_\wedge d * b) = g(da, b) - g(a, \delta b)$$

for all $a \in C^p(G/B)$, $b \in C^{p+1}(G/B)$, $0 \leqq p \leqq n$. Let us assume that $\dim H^n(G/B) = 1$. Then the exterior differential of any G-invariant $(n-1)$-form is zero and we have $g(da, b) = g(a, \delta b)$ for all $a \in C^p(G/B)$, $b \in C^{p+1}(G/B)$. If $b \in C^q(G/B)$, $q \neq p+1$, it is clear that $g(da, b) = g(a, \delta b) = 0$. Therefore we have $g(da, b) = g(a, \delta b)$ for all $a, b \in C^*(G/B)$. Moreover, we have $g(\Delta a, a) = g(da, da) + g(\delta a, \delta a)$. This equality shows that a G-invariant differential form a is harmonic if and only if $da = \delta a = 0$, in other words, if and only if a is orthogonal to the subspaces $dC^*(G/B)$ and $\delta C^*(G/B)$. On the other hand, the subspaces $dC^*(G/B)$ and $\delta C^*(G/B)$ are mutually orthogonal to each other. As is already mentioned, $C^*(G/B)$ is finite dimensional. Hence we obtain the proposition:

(5.2) *Let G/B be an n-dimensional Riemannian homogeneous space of a connected Lie group. If $H^n(G/B) \neq \{0\}$, any G-invariant form a on G/B has the unique decomposition $a = a_0 + a_1 + a_2$ such that a_0 is a G-invariant harmonic form, $a_1 \in dC^*(G/B)$ and $a_2 \in C^*(G/B)$.*

III. The Ricci curvature.

6. Let G/B be a reductive homogeneous space admitting a G-invariant Kaehlerian structure which is defined by the pair of an invariant complex structure I and an invariant Hermitian metric g. We take an ad B-stable decomposition $\mathfrak{g} = \mathfrak{b} + \mathfrak{m}$. The Ricci curvature r is equal to the canonical hermitian form defined by Koszul [6]. Hence the image $\pi^*\alpha$ of the Ricci form α is an exterior differential of a left invariant 1-form on G by a theorem of Koszul ([6], Theorem 1). We shall give a different approach to this fact from the view-point of differential geometry.

Let us consider the 1-form η in $C^*(G)$ given by

$$\eta(X)=-\mathrm{tr}_{\mathfrak{m}}\, I_\circ\cdot(\mathrm{ad}\, X_{\mathfrak{b}})_{\mathfrak{m}} \text{ for all } X\in g.$$

Since $I_\circ$ commutes with the restriction $(\mathrm{ad}\, b)_{\mathfrak{m}}$ of $\mathrm{ad}\, b$ on $\mathfrak{m}$ for all $b\in B$, we have

$$\begin{aligned}(\mathrm{ad}\, b\eta)(X)&=-\mathrm{tr}_{\mathfrak{m}}\, I_\circ.\,(\mathrm{ad}(\mathrm{ad}\, b\cdot X)_{\mathfrak{b}})_{\mathfrak{m}}\\ &=-\mathrm{tr}_{\mathfrak{m}}\,(\mathrm{ad}\, b)_{\mathfrak{m}},\cdot I_\circ\cdot(\mathrm{ad}\, X_{\mathfrak{b}})\cdot(\mathrm{ad}\, b)_{\mathfrak{m}}^{-1}=\eta(X),\end{aligned}$$

which implies that η is invariant by the right translation defined by any element in B. Since $\iota(X)d\eta+d\iota(X)\eta=\theta(X)\eta=0$ for all $X\in\mathfrak{b}$ and since $d\iota(X)\eta=0$ for all $X\in\mathfrak{b}$, we have $\iota(X)d\eta=0$ for all $X\in\mathfrak{b}$. It follows that $d\eta\in N^*(G:B)$. Moreover $d\eta$ belongs to $L^*(G/B)$, because $\mathrm{ad}\, b\cdot d\eta=d\,\mathrm{ad}\, b\cdot\eta=0$ for all $b\in B$. Next, let us consider the 1-form ξ in $N^*(G:B)$ defined by

$$\xi(X)=-\mathrm{tr}_{\mathfrak{m}}\, I_\circ\cdot D_{X_{\mathfrak{m}}} \quad \text{for all } X\in\mathfrak{g}.$$

Using (2.1) and the fact that $(\mathrm{ad}\, b)_{\mathfrak{m}}$, $b\in B$, commutes with $I_\circ$, we have

$$\begin{aligned}(\mathrm{ad}\, b\xi)(X)&=-\mathrm{tr}_{\mathfrak{m}} I_\circ\cdot D_{\mathrm{ad}\cdot b}X_{\mathfrak{m}}\\ &=-\mathrm{tr}_{\mathfrak{m}}(\mathrm{ad}\, b)_{\mathfrak{m}}\cdot I_\circ\cdot D_{X_{\mathfrak{m}}}\cdot(\mathrm{ad}\, b)_{\mathfrak{m}}^{-1}=\xi(X),\end{aligned}$$

which shows that ξ belongs to $L^1(G/B)$. Set $\phi=\eta+\xi$, then $d\phi\in L^2(G/B)$. By definition of the curvature tensor field R, we have

$$\begin{aligned}d\phi(X,Y)&=-\tfrac{1}{2}\phi([X,Y])=\tfrac{1}{2}\mathrm{tr}_{\mathfrak{m}}\, I_\circ\,(\mathrm{ad}[XY]_{\mathfrak{b}})_{\mathfrak{m}}+\tfrac{1}{2}\mathrm{tr}_{\mathfrak{m}}\, I_\circ D_{[X,Y]_{\mathfrak{m}}}\\ &=\tfrac{1}{2}\mathrm{tr}_{\mathfrak{m}}\, I_\circ\cdot(R(X,Y)-[D_X,D_Y])\end{aligned}$$

for all $X,Y\in\mathfrak{m}$. According to (2.5), we have

$$\mathrm{tr}_{\mathfrak{m}}\, I_\circ\cdot[D_X,D_Y]=\mathrm{tr}_{\mathfrak{m}}[I_\circ\cdot D_X,D_Y]=0.$$

Therefore we have $d\phi(X,Y)=\pi^*\alpha(X,Y)$ for all $X,Y\in\mathfrak{m}$. Since both $d\phi$ and $\pi^*\alpha$ are contained in $L^*(G/B)$, we have $d\phi=\pi^*\alpha$. Moreover, ξ being in $L^*(G/B)$, $\pi^*\alpha$ and $d\eta$ are cohomologous in $L^*(G/B)$. Thereby we have obtained the following proposition.

(6.1) *Let G/B be a reductive Kaehlerian homogeneous space of a connected Lie group G, and let $\mathfrak{g}=\mathfrak{b}+\mathfrak{m}$ be an $\mathrm{ad}\, B$-stable decomposition. The Ricci form α on G/B is cohomologous to the G-invariant 2-form ψ defined by*[2]

---

[2] Reading this manuscript, Koszul remarks that if a complex homogeneous space is reductive, the same result for the canonical Hermitian form is verified from his formula ([6], Theorem 1).

$$\psi_0(X,Y) = \mathrm{tr}_{\mathfrak{m}} I_0 \cdot (\mathrm{ad}[X,Y]_{\mathfrak{b}})_{\mathfrak{m}} \text{ for all } X, Y \in \mathfrak{m}.$$

We shall give a proof of the following fact:

(6.2) *The Ricci form α on a Kaehlerian homogeneous space is harmonic* [7].

Since the fact that the Ricci form is harmonic does not depend upon the Lie group acting transitively on the space, we can assume the homogeneous G/B to be reductive on account of (1,1). Therefore, applying the fact that $\pi^*\alpha = d\phi$, we have $d\alpha = 0$.

Let $\{X_1, \cdots, X_m, IX_1, \cdots, IX_m\}$ be an orthogonal frame defined on an arbitrary open set. We set $Z_\alpha = X_\alpha + (-1)^{\frac{1}{2}} IX_\alpha$, $Z_{\alpha^*} = X_\alpha - (-1)^{\frac{1}{2}} IX_\alpha$, $1 \leqq \alpha \leqq m$. Since $\alpha(IX, IY) = \alpha(X, Y)$ for all vector fields X, Y, we have $\alpha(Z_\alpha, Z_\beta) = \alpha(Z_{\alpha^*}, Z_{\beta^*}) = 0$, $1 \leqq \alpha, \beta \leqq m$. Moreover, $\sum_{1 \leqq \alpha \leqq m} \alpha(Z_\alpha, Z_{\alpha^*})$ is a constant over the open set, because the scalar $\sum_{1 \leqq \alpha \leqq m} \alpha(Z_\alpha, Z_{\alpha^*})$ is invariant by G. From the fact that $d\alpha = 0$, we have

$$\begin{aligned} 0 &= (d\alpha)(Z_\beta, Z_\alpha, Z_{\alpha^*}) \\ &= \tfrac{1}{3}((\nabla_{Z_\beta}\alpha)(Z_\alpha, Z_{\alpha^*}) + (\nabla_{Z_\alpha}\alpha)(Z_{\alpha^*}, Z_\beta) + (\nabla_{Z_{\alpha^*}}\alpha)(Z_\beta, Z_\alpha)). \end{aligned}$$

It follows that $(\nabla_{Z_\alpha}\alpha)(Z_{\alpha^*}, Z_\beta) = -(\nabla_{Z_\beta}\alpha)(Z_\alpha, Z_{\alpha^*})$, $1 \leqq \alpha, \beta \leqq m$. Using this, we have

$$\begin{aligned} (\delta\alpha)(Z_\beta) &= -\tfrac{1}{2} \sum_{1 \leqq \alpha \leqq m} ((\nabla_{Z_\alpha}\alpha)(Z_{\alpha^*}, Z_\beta) + (\nabla_{Z_{\alpha^*}}\alpha)(Z_\alpha, Z_\beta)) \\ &= -\tfrac{1}{2} \sum_{1 \leqq \alpha \leqq m} (\nabla_{Z_\beta}\alpha)(Z_\alpha, Z_{\alpha^*}) = 0, \qquad 1 \leqq \beta \leqq m. \end{aligned}$$

By the same argument, we have $(\delta\alpha)(Z_{\beta^*}) = 0$, $1 \leqq \beta \leqq m$. Thus we have $\delta\alpha = 0$ and $\Delta\alpha = (d\delta + \delta d)\alpha = 0$, completing the proof.

IV. Theorems.

7. When a homogeneous space G/B has a G-invariant and non-degenerate 2-cocycle Ω, we say an invariant symplectic structure is defined on G/B. If G/B admits an invariant Kaehlerian structure, the Kaehlerian form Ω defines an invariant symplectic structure. When G/B has an invariant symplectic structure defined by a 2-cocycle Ω, the dimension of G/B is an even integer $2m$ and Ω^m, the Grassmann m-th power of Ω, is not zero. In general, an exterior form Ω of degree 2 on a real $2m$-dimensional vector space is non-degenerate if and only if $\Omega^m \neq 0$.

The purpose of this section is to prove the following:

LEMMA 1. *Let G be a connected Lie group and let B be a closed connected semi-simple subgroup of G. If the homogeneous space G/B admits an invariant symplectic structure and if $H^{2m}(G/B) = 0$, where $2m = \dim G/B$, then B is a maximal connected semi-simple subgroup of G.*[3]

Let Ω be a G-invariant 2-cocycle on G/B defining the invariant symplectic structure. We denote by h the left invariant 2-cocycle $\pi^*\Omega$ on G. Since Ω is non-degenerate, we see that an element X of $\mathfrak{g}$ belongs to $\mathfrak{b}$ if and only if $h(X, Y) = 0$ for all $Y \in g$. Let S be a maximal connected semi-simple subgroup containing B.

In order to prove the lemma, we introduce a filtration in $C^*(G)$ by means of S. We denote by C^p the ideal in $C^*(G)$ generated by $N^p(G:S)$. The sequence $C^*(G) = C^0 \supset C^1 \supset \cdots \supset C^p \supset \cdots$ defines a filtration in $C^*(G)$. Let $Z^p{}_s$ be the set of all elements $a \in C^p$ such that $da \in C^{p+s}$, and put $dZ^{p-s}{}_s = D^p{}_s$. Then $Z^{p+1}{}_{s-1} + D^p{}_{s-1}$ is an ideal of $Z^p{}_s$. We denote by $E^p{}_s$ the factor algebra $Z^p{}_s/Z^{p+1}{}_{s-1}$ and by $\eta^p{}_s$ the natural projection from $Z^p{}_s$ onto $E^p{}_s$. Let $E^{q,p}{}_s$ be the subspace of $E^p{}_s$ consisting of all elements which are images of elements of degree $p + q$ in $Z^p{}_s$. As for $E^{q,p}{}_1$, it is known from a theorem of Koszul ([5], Theorem 15.2) that there is an isomorphism from $H^q(S) \otimes L^p(G:S)$ onto $E^{q,p}{}_1$, where $H^q(S)$ is the q-homogeneous part of the cohomology algebra $H^*(S)$. Since S is semi-simple, we have $H^1(S) = H^2(S) = \{0\}$. It follows that $E^{1,p}{}_1 = E^{2,p}{}_1 = \{0\}$, $0 \leqq p$.

Since the form h is a cocycle, h belongs to $Z^0{}_s$ for any s. Since the degree of h is two, we have $\eta^0{}_1 h \in E^{2,0}{}_1$. Hence we have $\eta^0{}_1 h = 0$, which shows that $h \in Z^1{}_0 + D^0{}_0$ that is, h is cohomologous to an element $h' \in Z^1{}_0$. The form h' being a cocycle in $Z^1{}_0$, we have $h' \in Z^1{}_s$ for all s. From the facts that $E^{1,1} = \{0\}$ and that $\eta^1{}_1 h' \in E^{1,1}{}_1$, we have $\eta^1{}_1 h' = 0$ and $h' \in Z^2{}_0 + D^1{}_0$. Hence h' is cohomologous to an element $h'' \in Z^2{}_0$. Since the degree of h'' is two, h'' is in $N^2(G:S)$. Moreover, h'' being a cocycle, we have $\theta(X)h'' = \iota(X)dh'' + d\iota(X)h'' = 0$ for all $X \in \mathfrak{s}$, where $\mathfrak{s}$ denotes the subalgebras of $\mathfrak{g}$ corresponding to S. Therefore h'' belongs to $L^2(G:S)$. It follows that the cocycle h is cohomologous to the cocycle h'' which is in $L^2(G:S)$, that is, $h - h'' = da$ for a certain $a \in C^1(G)$.

Next we shall prove that h and h'' are cohomologous to each other in $L^*(G:B)$. For this purpose, it is sufficient to show that a is contained in $L^*(G:B)$. Since $B \subset S$, we have $L^*(G:B) \supset L^*(G:S)$, and so h'' and da are in $L^2(G:B)$. Hence we have $\theta(X)a = \iota(X)da + d\iota(X)a = 0$ for all

---

[3] First the author dealt with the case where the isotopy group $B = \{e\}$. The generalization is due to Matsushima.

$X\in\mathfrak{b}$, that is, $a([X,Y])=0$ for all $X\in\mathfrak{b}$ and $Y\in\mathfrak{g}$. Since $\mathfrak{b}$ is semi-simple, the derived algebra $[\mathfrak{b},\mathfrak{b}]$ of $\mathfrak{b}$ coincides with $\mathfrak{b}$. Therefore we have $\iota(X)a=0$ for all $X\in\mathfrak{b}$, and so we have $a\in L^2(G:B)$.

From our assumption, the $2m$-cocycle h^m is not zero. Hence h^m is not cohomologous to zero in $L^*(G:B)$. This follows from our assumption that $H^{2m}(G/B)\neq\{0\}$ and from the fact that G is connected. Suppose that $\mathfrak{b}$ were not equal to $\mathfrak{s}$, and let X_0 be an element of $\mathfrak{s}$ not contained in $\mathfrak{b}$. Since $h''\in L^*(G:S)$, we would have $(\iota(X_0)h'')(Y)=\frac{1}{2}h''(X_0,Y)=0$ for all $Y\in\mathfrak{g}$ and accordingly $h''^m=0$. On the other hand, h'' and h''^m are cohomologous to each other in $L^*(G:b)$. This is impossible and hence we have $\mathfrak{b}=\mathfrak{s}$, which implies $B=S$. Thus the proof is completed.

8. In this section we prepare two lemmas for the first theorem.

LEMMA 2. *Let G/B be a Kaehlerian homogeneous space of dimension $2m$. If B is a connected semi-simple subgroup, and if $H^{2m}(G/B)\neq\{0\}$, then the Ricci curvature r is zero.*

From our assumption that B is a connected semi-simple subgroup; G/B is a reductive homogeneous space; let $\mathfrak{g}=\mathfrak{b}+\mathfrak{m}$ be an $\mathrm{ad}\,B$-stable decomposition. Let us consider the complexification $\mathfrak{m}^c$ of $\mathfrak{m}$, and let $\mathfrak{m}^+$ (resp. $\mathfrak{m}^-$) be the complex subspace spanned by all vectors $X-(-1)^{\frac{1}{2}}I_\circ X$ (resp. $X+(-1)^{\frac{1}{2}}I_\circ X$), $X\in\mathfrak{m}$. The space $\mathfrak{m}^+$ and $\mathfrak{m}^-$ are eigenspaces of $I_\circ$ belonging to the eigenvalues $(-1)^{\frac{1}{2}}$ and $-(-1)^{\frac{1}{2}}$ respectively. If $X\in\mathfrak{b}$, $(\mathrm{ad}\,X)_{\mathfrak{m}}$ commutes with $I_\circ$ and so leaves $\mathfrak{m}^+$ and $\mathfrak{m}^-$ stable respectively. Hence we have two representations of the subalgebra $\mathfrak{b}$ given by $X\to(\mathrm{ad}\,X)_{\mathfrak{m}^+}$ and $X\to(\mathrm{ad}\,X)_{\mathfrak{m}^-}$; these representations are mutually conjugate. Recalling that $(\mathrm{ad}\,X)_{\mathfrak{m}}$ is skew symmetric with respect to the inner product $g_\circ$ on $\mathfrak{m}$, we have $\mathrm{tr}_{\mathfrak{m}} I_\circ\cdot(\mathrm{ad}\,X)_{\mathfrak{m}}=2(-1)^{\frac{1}{2}}\mathrm{tr}_{\mathfrak{m}^+}(\mathrm{ad}\,X)_{\mathfrak{m}^+}$ for all $X\in\mathfrak{b}$. Furthermore, since $\mathfrak{b}$ is semi-simple, we have $\mathrm{tr}_{\mathfrak{m}^+}(\mathrm{ad}\,X)_{\mathfrak{m}^+}=0$ for all $X\in\mathfrak{b}$. Thus we have $\mathrm{tr}_{\mathfrak{m}} I_\circ\cdot(\mathrm{ad}\,X)_{\mathfrak{m}}=0$ for all $X\in\mathfrak{b}$, which implies

$$\psi_\circ(X,Y)=\mathrm{tr}_{\mathfrak{m}}\,I_\circ\cdot(\mathrm{ad}\,X)_{\mathfrak{m}}=0$$

for all $X,Y\in\mathfrak{m}$. In virtue of (6.1), the Ricci form α is cohomologous to zero. On the other hand α is a harmonic form by (6.2). Accordingly we have $\alpha=0$ by proposition (5.2), completing the proof.

LEMMA 3. *Let G/B be a Riemannian homogeneous space on which G acts effectively. If the restricted homogeneous holonomy group is irreducible and if the Ricci curvature is zero, then the group G is unimodular.*

Let us consider the left invariant 1-form t on G defined by $t(X) = \mathrm{tr}_{\mathfrak{g}}\,\mathrm{ad}\,X$ for all $X \in \mathfrak{g}$. Obviously t is also right invariant and we have $dt = 0$. Since G is effective on G/B, $\mathrm{ad}\,X$, $X \in \mathfrak{b}$, is skew symmetric with respect to an inner product of $\mathfrak{g}$ by the argument in **1**. Hence we have $t(X) = 0$ for all $X \in \mathfrak{b}$. These facts show that the 1-cocycle t is contained in $L^1(G/B)$, and there is a G-invariant 1-cocycle τ on G/B such that $\pi^*\tau = t$. We have $\Delta\tau = d\delta\tau + \delta d\tau = 0$, because $\delta\tau$ is a constant over G/B. Since the Ricci curvature is zero, we see that τ is a parallel field, on account of (5.1). As we assume that the restricted homogeneous holonomy group is irreducible, we can conclude that either t is zero or the dimension of G/B is equal to one. In the second case G is a 1-dimensional abelian group. In any case, the group G is unimodular. We have completed the proof.

9. We shall prove the following

THEOREM 1. *Let G/B be a Kaehlerian homogeneous space of dimension $2m$. If B is a connected semi-simple subgroup and if $H^{2m}(G/B) \neq \{0\}$, then the restricted homogeneous holonomy group reduces to the identity group.*

Since the Kaehlerian form Ω defines an invariant symplectic structure on G/B, B is a maximal connected semi-simple subgroup of G by Lemma 1. Let R be the radical of G, that is, the maximal connected solvable normal subgroup of G. Then by a well known theorem of Levi-Malcev, we have $G = B \cdot R$ and $B \cap R$ is a discrete normal subgroup, which we denote by D. Hence the solvable group R is transitive on G/B and the isotropy group of o is equal to D. We have a left invariant Kaehlerian structure on the group R which is locally isomorphic with given one on G/B by the projection from R onto G/B. By Lemma 2, the Ricci curvature of G/B is zero and accordingly the Ricci curvature of R is also zero. Therefore, in order to complete the proof, it is sufficient to prove the following

LEMMA 4. *Let G be a connected solvable Lie group. If the Ricci curvature of a left invariant Riemannian metric is zero, then the restricted homogeneous holonomy group is equal to $\{e\}$.*

We take the universal covering group of G, then this space has a left invariant Riemannian metric naturally induced by that of G and the projection is locally isometric. Therefore, for our purpose, we have only to prove that the homogeneous holonomy group reduces to $\{e\}$, when the group G is simply connected. Let $G = G_0 \times G_1 \times \cdots \times G_s$ be the canonical decomposition with respect to the homogeneous holonomy group. Each component G_i is also a solvable Lie group and its Riemannian metric is left invariant. Moreover, the Ricci curvature r_i on G_i is equal to zero. We shall show that the subgroups G_i, $1 \leqq i \leqq s$ do not appear in the decomposition, which means that the homogeneous holonomy group of the Riemannian space G is equal to $\{e\}$.

Assume that, say, $\dim G_1 = n_1 > 0$. Since the space G_1 is irreducible and since the Ricci curvature r_1 is zero, the group G_1 is unimodular by Lemma 3 and then we have $H^{n_1}(G) \neq \{0\}$. Since the Lie algebra $\mathfrak{g}_1$ of G_1 is a non-zero solvable algebra, the dimension of the derived algebra $\mathfrak{g}_1'$ is less than that of $\mathfrak{g}_1$. It follows that $\dim H^1(G_1) = \dim \mathfrak{g}_1 - \dim \mathfrak{g}_1' \neq 0$. In virtue of (5.2), the dimension of $H^1(G_1)$ is equal to that of the space of all left invariant harmonic forms of degree 1. Therefore, there is a non-zero harmonic form of degree 1. Therefore, there is a non-zero harmonic form a. By proposition (5.1), a is a parallel field. Since the homogeneous holonomy group is irreducible, we have $\dim G_1 = 1$, which is impossible. Thereby. we have proved the lemma and completed the proof of Theorem 1.

Now, we shall clarify the algebraic structure of solvable Lie groups G which admit a locally flat Riemannian connection. Since the curvature tensor R is zero, we have $[D_X, D_Y] = D_{[X,Y]}$ for all $X, Y \in \mathfrak{g}$ by (2.3). The correspondence $X \rightarrow D_X$ gives a representation of the Lie algebra $\mathfrak{g}$. By a well known theorem of Lie, the derived algebra of a linear solvable Lie algebra consists of nilpotent linear mappings. Therefore D is nipotent for all $X \in \mathfrak{g}'$, where $\mathfrak{g}'$ is the derived algebra of $\mathfrak{g}$. On the other hand, D_X is a skew symmetric linear mapping with respect to the inner product g by (2.2), and hence we have $D_X = 0$ for all $X \in \mathfrak{g}'$. If $X, Y \in \mathfrak{g}'$, we have $[X, Y] = D_X Y - D_Y X = 0$, which shows that $\mathfrak{g}'$ is abelian. Thus we have shown that the group G is meta-abelian. Let $\mathfrak{h}$ be the orthogonal complement of $\mathfrak{g}'$ with respect to the inner product g. If $X \in \mathfrak{h}$ and $Y \in \mathfrak{g}'$, we have $[X, Y] = D_X Y - D_Y X = D_X Y$. Since $\mathfrak{g}'$ is an ideal, we have $D_X Y \in \mathfrak{g}'$. Hence we see that $\mathfrak{g}'$ and accordingly $\mathfrak{h}$ are stable by D_X for all $X \in \mathfrak{h}$, and that $\operatorname{ad} X$ and D_X induce the same linear mapping on $\mathfrak{g}'$ for all $X \in \mathfrak{h}$. It follows that if $X, Y \in \mathfrak{h}$, $[X, Y] = D_X Y - D_Y X \in \mathfrak{h}$. On the other hand we have $[\mathfrak{h}, \mathfrak{h}] \subset \mathfrak{g}'$. According we have $[\mathfrak{h}, \mathfrak{h}] = 0$.

Now, let us assume that $\mathfrak{g}$ is nilpotent. Then $\operatorname{ad} X$ is nilpotent for all $X \in \mathfrak{g}$. If $X \in \mathfrak{h}$, the restriction on $\mathfrak{g}'$ of $\operatorname{ad} X$, which coincides with that of D_X, is simultaneously nilpotent and skew symmetric and accordingly is equal to zero. Hence we have $[\mathfrak{h}, \mathfrak{g}'] = 0$. After all we have proved that $\mathfrak{g}$ is abelian. From these considerations we have

THEOREM 2. *If a unimodular Lie group G admits a left invariant Kaehlerian structure, then the restricted homogeneous holonomy group is equal to $\{e\}$ and the group G is meta-abelian. Especially if the group G is nilpotent, then it must be abelian.*

If a Lie group G admits a left invariant Kaehlerian structure whose Ricci curvature is zero, then we have the same conclusion as above on account of Lemma 4.

10. We now prove the following

THEOREM 3. *Let G/B be a $2m$-dimensional Kaehlerian homogeneous space having the non-degenerate Ricci curvature. If G acts effectively on G/B and if $H^{2m}(G/B) \neq \{0\}$, then the group G is semi-simple.*

Since G is effective on G/B, the subgroup B is reductive in G by (1.1), and if $b \in B$, $\operatorname{ad} b$ is orthogonal with respect to a certain positive definite symmetric bilinear form on $\mathfrak{g}$. Let $\mathfrak{g} = \mathfrak{b} + \mathfrak{m}$ be an $\operatorname{ad} B$-stable decomposition of $\mathfrak{g}$.

Since the Ricci curvature is non-degenerate, so is the Ricci form α. Hence we have $\alpha^m \neq 0$, which shows that α^m is not cohomologous to zero on account of our assumption that $H^{2m}(G/B) \neq \{0\}$. By (6.1), the cocycle α is cohomologous to the G-invariant cocycle ψ defined by

$$\psi_\circ(X, Y) = \operatorname{tr}_{\mathfrak{m}} I_\circ \cdot (\operatorname{ad}[X, Y]_{\mathfrak{b}})_{\mathfrak{m}}$$

for all $X, Y \in \mathfrak{m}$. Hence ψ^m, being cohomologous to α^m, is not cohomologous to zero, and a fortiori, ψ^m is not zero. Thus we see that ψ is non-degenerate, that is $\operatorname{tr}_{\mathfrak{m}} I_\circ \cdot (\operatorname{ad}[X, Y]_{\mathfrak{b}})_{\mathfrak{m}} = 0$ for all $Y \in \mathfrak{m}$, if and only if $X = 0$.

Let $\mathfrak{a}$ be an arbitrary abelian ideal of $\mathfrak{g}$. If $X \in \mathfrak{a}$, $\operatorname{ad} X$ is a nilpotent linear mapping. We can easily verify that $\mathfrak{a} \cap \mathfrak{b} = \{0\}$. In fact, if an element X is contained in $\mathfrak{a} \cap \mathfrak{b}$, $\operatorname{ad} X$ is simultaneously skew symmetric and nilpotent. Hence we have $\operatorname{ad} X = 0$ for all $X \in \mathfrak{a} \cap \mathfrak{b}$ which implies that $\mathfrak{a} \cap \mathfrak{b}$ is an ideal contained in the center of $\mathfrak{g}$. Since G is effective on G/B, the subalgebra $\mathfrak{b}$ cannot contain any ideal of $\mathfrak{g}$ except the zero ideal, and hence we have $\mathfrak{a} \cap \mathfrak{b} = \{0\}$. Since the subgroup B is reductive in G, we can take an $\operatorname{ad} B$-stable decomposition $\mathfrak{g} = \mathfrak{b} + \mathfrak{m}$ such that $\mathfrak{m}$ contains $\mathfrak{a}$. Let us apply the above consideration to this decomposition. If $X \in \mathfrak{a}$ and $Y \in \mathfrak{g}$, $[X, Y]$ belongs to $\mathfrak{a}$ and hence we have $[X, Y]_{\mathfrak{b}} = 0$. It follows that if $X \in \mathfrak{a}$, $\operatorname{tr}_{\mathfrak{m}} I_\circ \cdot (\operatorname{ad}[X, Y]_{\mathfrak{b}})_{\mathfrak{m}} = 0$ for all $Y \in \mathfrak{m}$, which shows that $\mathfrak{a} = \{0\}$.

Thus we have seen that any abelian ideal in $\mathfrak{g}$ reduces to $\{0\}$, and accordingly the algebra $\mathfrak{g}$ is semi-simple, which completes the proof.

NAGOYA UNIVERSITY.

REFERENCES.

[1] A. Borel, "Kaehlerian coset spaces of semi-simple Lie groups," *Proceedings of the National Academy of Science, U. S. A.*, vol. 40 (1954), pp. 1147-1151.

[2] E. Cartan, "Sur les domaines bornés homogènes de l'espace de *n* variables complexes," *Abh. Math. Seminar Hamburg*, vol. 11 (1935), pp. 116-162.

[3] G. de Rham, "Sur la réductibilité d'un espace de Riemann," *Comm. Math. Helv.*, vol. 26 (1952), pp. 328-344.

[4] ———, *Variétés Différentiables*, Hermann, Paris (1955).

[5] J. L. Koszul, "Homologie et cohomologie des algèbres de Lie," *Bulletin Soc. Math. France*, vol. 78 (1950), pp. 65-127.

[6] ———, "Sur la forme hermitienne canonique des espace homogènes complexes," *Canadian Journal of Mathematics*, vol. 7 (1955), pp. 562-576.

[7] A. Lichnerowicz, "Espaces homogènes kaehlériens," *Coll. Géom. Diff.* (Strasbourg, 1953), pp. 171-184.

[8] Y. Matsushima, "Sur les espaces homogènes kaehlériens d'un groupe de Lie réductif," *Nagoya Mathematical Journal*, vol. 11 (1957), pp. 53-60.

[9] K. Nomizu, "Invariant affine connections on homogeneous spaces," *American Journal of Mathematics*, vol. 76 (1954), pp. 33-65.

[10] ———, "Studies on Riemannian homogeneous spaces," *Nagoya Mathematical Journal*, vol. 9 (1955), pp. 43-56.

SINGULAR INTEGRAL OPERATORS AND DIFFERENTIAL EQUATIONS.*[1]

By A. P. CALDERÓN and A. ZYGMUND.

1. Introduction. Let $P(u)$ be a linear partial differential operator with smooth coefficients and of homogeneous order m. Then $P = H\Lambda^m$ where Λ is a square root of the Laplacian (see definition [1] below) and H is a singular integral operator (see Theorem 7). This fact seems to call for a closer study of the properties of singular integral operators in their connection with the operator Λ and supplies the subject matter of the present paper.

Our results can be briefly summarized as follows. With each singular integral operator there is associated a function (its "symbol" in the terminology of Giraud and Mihlin) in a one-to-one fashion. This correspondence is linear and pseudo-multiplicative in the sense that, modulo a class of regular operators, singular integral operators can be multiplied (in the sense of operator composition) by simply multiplying their symbols. The regular operators in that class have the property of remaining bounded after being multiplied on the left or on the right by Λ. An algebraic formulation of these facts will be found in Theorem 6. The reader familiar with the work of Giraud, Mihlin and Tricomi[1a] will recognize the similarity of some of our results with theirs. The main distinctive feature is that we are concerned with the operator Λ which they do not consider, and that our operators act on L^p, $1 < p < \infty$, instead of on L^2 only. For many applications, though, it suffices to consider the case of L^2, and, in this respect and as far as mean convergence of the singular integrals goes, the paper is self-contained. To conclude these preliminary remarks, we want to stress the fact that many of the assumptions on which our results are obtained can be considerably relaxed. Since these improvements do not seem to be of particular relevance at the present time, we prefer not to burden the reader and postpone their discussion to another opportunity.

---

* Received June 12, 1957.

[1] This research was partly supported by the United States Air Force under contract No. AF18(600)-685 monitored by the Office of Scientific Research.

[1a] A description of the work of these authors can be found in the paper "Singular integral equations" by S. G. Mihlin, Uspekhi Matematicheskikh Nauk, No. 25 (1948), 29-112.

2. Definitions and notation. We will be concerned with functions defined in the k-dimensional Euclidean space E_k. Points in E_k will be denoted by $x = (x_1, \cdots, x_k)$, $y = (y_1, \cdots, y_k)$ etc. and we will use the following abbreviations $|x| = [\sum_1^k x_i^2]^{\frac{1}{2}}$, $\lambda x = (\lambda x_1, \cdots, \lambda x_k)$, $x' = x\,|x|^{-1}$, $x + y = (x_1 + y_1, \cdots, x_k + y_k)$, $x \cdot y = \sum_1^k x_i y_i$. The sphere $|x| = 1$ in E_k will be denoted by Σ, the element of surface area on Σ by $d\sigma$, and dx will stand for the volume element in E_k. By C_α, $\alpha \geqq 0$, we shall denote the class of complex valued continuous bounded functions on E_k with bounded continuous derivatives up to order $[\alpha]$ (integral part of α) and with derivatives of order $[\alpha]$ satisfying a (uniform) Hölder condition of order $\alpha - [\alpha]$. When dealing with functions depending on more than one argument, we will denote by C_α^∞ the class of functions in C_α which are in C^∞ with respect to the last argument and whose derivatives of all orders with respect to variables in the last argument are in C_α. Given a subclass of C_α or C_α^∞, we shall say that the subclass is uniform if the bounds and Hölder conditions on the functions and their derivatives are uniform in the subclass.

We shall also consider the class L_r^p of functions in $L^p(E_k)$ with derivatives up to order r in $L^p(E_k)$. The notion of derivative used here is that of Schwartz; that is, $g = \partial f/\partial x_i$ means $(f, \partial\phi/\partial x_i) = -(g, \phi)$ for every $\phi \in C^\infty$ vanishing outside a bounded set, where here, as in the rest of the paper, (f, g) stands for the integral of $f\bar{g}$ over E_k. By A and C we will denote constants, though they will not be necessarily the same in different occurrences.

3. In this section we shall establish some properties of expansions of functions in spherical harmonics. Let $Y_n(x')$ be a normalized real spherical harmonic of degree n, that is, such that

$$\int_\Sigma Y_n(x')^2 . d\sigma = 1$$

and $Y_{nm}(x')$, $m = 1, 2, \cdots$, a complete orthogonal system of normalized harmonics of degree n. Our first objective is to obtain bounds for the $Y_n(x')$ and their successive derivatives. Consider first the case $k \geqq 3$. Then we have the formula (see [4])

$$(1) \qquad \delta_{nm} Y_m(x') = \tfrac{1}{2}\Gamma(\lambda)(n+\lambda)/\pi^{\lambda+1} \int_\Sigma P_n^\lambda(x' \cdot y') Y_n(y')\, d\sigma$$

where $\lambda = \frac{1}{2}(k-2)$, δ_{nm} is Kronecker's delta and $P_n^\lambda(t)$ is the ultraspherical polynomial defined by

$$(1 - 2wt + w^2)^{-\lambda} = \sum_0^\infty w^n P_n^\lambda(t). \tag{2}$$

For each z, the function $P_n^\lambda(x' \cdot z')$ is a spherical harmonic of degree n, whence, replacing in (1) and setting $x' = z'$, we obtain

$$P_n^\lambda(1) = \tfrac{1}{2}\Gamma(\lambda)(n + \lambda)/\pi^{\lambda+1} \int_\Sigma P_n(y' \cdot z')^2 \, d\sigma.$$

On the other hand, from (2) it follows that

$$(1 - w)^{-k+2} = \sum_0^\infty w^n P_n^\lambda(1),$$

which implies that $P_n^\lambda(1)$ is of the order n^{k-3} as $n \to \infty$. Hence

$$\int_\Sigma P_n^\lambda(y' \cdot z')^2 \, d\sigma$$

is of order n^{k-4}, and Schwarz's inequality applied to (1) gives

$$|Y_n(x')| \leqq C n^{\frac{1}{2}(k-2)}, \qquad n \geqq 1, \tag{3}$$

where C is a constant depending only on k. In order to estimate the derivatives of $Y_n(x')$, let $P_n(x)$ denote temporarily the solid harmonic coinciding with $Y_n(x')$ on Σ. Then, if S denotes the sphere $|x| \leqq 1$ and $\partial P_n/\partial \nu$ is the derivative of P_n in the direction of the outer normal to the boundary Σ of S, we have

$$\int_\Sigma P_n(\partial P_n/\partial \nu) \, d\sigma = \int_S |\operatorname{grad} P_n|^2 \, dx.$$

Now P_n and $|\operatorname{grad} P_n|^2$ are homogeneous functions of degrees n and $2n - 2$, respectively, and from this it follows readily that the two integrals are respectively equal to

$$n \int_\Sigma P_n^2 \, d\sigma = n \text{ and } (2n + k - 2)^{-1} \int_\Sigma |\operatorname{grad} P_n|^2 \, d\sigma,$$

which implies that

$$\int_\Sigma |\partial P_n/\partial x_i|^2 \, d\sigma \leqq C n^2.$$

But $\partial P_n/\partial x_i$ is a homogeneous harmonic polynomial of degree $n - 1$, and therefore we can write $\partial P_n/\partial x_i = \lambda P_{n-1}$, where P_{n-1} is a solid harmonic coinciding with a normalized spherical harmonic of degree $n - 1$ on Σ, and $|\lambda| \leqq Cn$.

Now we write $Y_n(x') = |x|^{-n} P_n(x)$, and by differentiating and applying (3) and the formula above to the successive derivatives of P_n, we obtain

$$|D_r Y_n(x')| \leqq C n^{\frac{1}{2}(k-2)+r}, \qquad |x| \geqq 1, \tag{4}$$

where $D_r Y_n$ denotes a derivative of Y_n of order r and C is a constant depending on r and k. If $k = 2$, a normalized spherical harmonic is the real part of $\pi^{-\frac{1}{2}} e^{i\theta}(w\,|w|^{-1})^n$, where $w = x_1 + ix_2$ and θ is a real number. Clearly (3) still holds in this case and (4) is obtained by differentiation.

Our next step will be to establish the formula (8) for the coefficients of the expansion of a function in spherical harmonics.

Let $F(x) = F(x')$, $G(x) = G(x')$ be two homogeneous functions of degree zero, and let S_ϵ be the spherical shell between the spheres of radii 1 $1 + \epsilon$. Since F and G are homogeneous of degree zero, their normal derivatives at points of the boundary of S_ϵ are zero. Consequently, if we apply Green's formula to the pair F, G, the surface integral vanishes and we obtain

$$\int_{S_\epsilon} F \Delta G\, dx = \int_{S_\epsilon} G \Delta F\, dx;$$

dividing by ϵ and letting ϵ tend to zero it follows that

$$\int_\Sigma F \Delta G\, d\sigma = \int_\Sigma G \Delta F\, d\sigma.$$

If we define now

$$L(F) = |x|^2 \Delta F(x), \tag{5}$$

then, since $|x| = 1$ on Σ, it follows that

$$\int_\Sigma F L(G)\, d\sigma = \int_\Sigma G L(F)\, d\sigma.$$

But if F is homogeneous of degree zero, so is $L(F)$, and a repeated application of the last formula gives

$$\int_\Sigma F L^r(G)\, d\sigma = \int_\Sigma G L^r(F)\, d\sigma \tag{6}$$

which holds, of course, if F and G have sufficiently many continuous derivatives in $|x| > 0$.

Let us consider now a spherical harmonic $Y_{nm}(x')$. Then $|x|^n Y_{nm}(x')$ is a solid harmonic and its Laplacian vanishes. Since the gradients of $Y_{nm}(x')$ and $|x|^n$ are mutually orthogonal, we have that

$$0 = \Delta[|x|^n Y_{nm}(x')] = |x|^n \Delta Y_{nm} + n(n+k-2)\,|x|^{n-2} Y_{nm};$$

whence, we obtain

$$L[Y_{nm}(x')] = -n(n+k-2)\,Y_{nm}(x'). \tag{7}$$

Let now $F(x')$ be a homogeneous function of degree zero and let

$$F(x') = a_0 + \sum_{n\geqq 1} a_{nm} Y_{nm}(x')$$

be its expansion in spherical harmonics. Then

$$a_{nm} = \int_\Sigma F(x') Y_{nm}(x')\,d\sigma, \qquad n \geqq 1,$$

and an application of (7) and (6) to the last integral gives

$$a_{nm} = (-1)^r n^{-r} (n+k-2)^{-r} \int_\Sigma L^r(F) Y_{nm}(x')\,d\sigma, \qquad n \geqq 1. \tag{8}$$

Now we shall compute compute the Fourier transforms of homogeneous functions coinciding with a normalized spherical harmonic on Σ. Let us write

$$\begin{aligned} Y_{nm}(\epsilon,\delta,x) &= \begin{cases} Y_{nm}(x')\,|x|^{-k} & \text{if } \epsilon \leqq |x| \leqq \delta, \\ 0 & \text{otherwise,} \end{cases} \\ Y_{nm}(\epsilon,x) &= \begin{cases} Y_{nm}(x')\,|x|^{-k} & \text{if } \epsilon \leqq |x|, \\ 0 & \text{otherwise.} \end{cases} \end{aligned} \tag{9}$$

Then

$$\hat{Y}_{nm}(\epsilon,\delta,x) = \int_{\epsilon\leqq|y|\leqq\delta} e^{i(x\cdot y)} Y_{nm}(y')\,|y|^{-k}\,dy$$

Now we set $r = |x|$, $\rho = |y|$ and denote by γ the angle between x and y, and the integral above becomes

$$\begin{aligned} &\int e^{ir\rho\cos\gamma} Y_{nm}(y')\,|y|^{-k}\,dy \\ &= \int_\epsilon^\delta d\rho/\rho \int_\Sigma e^{ir\rho\cos\gamma} Y_{nm}(y')\,d\sigma = \int_{\epsilon r}^{\delta r} ds/s \int_\Sigma e^{is\cos\gamma} Y_{nm}(y')\,d\sigma, \end{aligned} \tag{10}$$

and since the integral of Y_{nm} over Σ is zero, the last integral can be written as

$$\begin{aligned} &\int_{\epsilon r}^{\delta r} ds/s \int_\Sigma (e^{is\cos\gamma} - e^{-s})\,Y_{nm}(y')\,d\sigma \\ &\qquad = \int_\Sigma Y_{nm}(y') \left[\int_{\epsilon r}^{\delta r} (e^{is\cos\gamma} - e^{-s})/s\,ds\right] d\sigma. \end{aligned}$$

Now the inner integral can be estimated readily by integrating between ϵr and 1, and 1 and δr, and one verifies that it is dominated in absolute value by $\log C/|\cos\gamma|$ and that it converges as $\epsilon \to 0$ and $\delta \to \infty$. Hence, applying Schwarz's inequality to the last integral, we obtain

$$|\hat{Y}_{nm}(\epsilon,\delta,x)| \leqq C, \qquad |\hat{Y}_{nm}(\epsilon,x)| \leqq C, \tag{11}$$

where C depends only on k. Further, as $\epsilon \to 0$ and $\delta \to \infty$, both functions converge to the same limit which we shall denote by $\hat{Y}_{nm}(x)$.

Now we wish to obtain an explicit expression for $\hat{Y}_{nm}(x)$ (see also [2]). For this purpose, let us revert to (10) and assume first that $k \geqq 3$. Then from the expansion

$$e^{is\cos\gamma} = 2^{\lambda}\Gamma(\lambda) \sum_{n=0}^{\infty} (n+\lambda) i^n J_{n+\lambda}(s)/s^{\lambda} P_n{}^{\lambda}(\cos\gamma), \qquad \lambda = \tfrac{1}{2}(k-2),$$

where J_k is Bessel's function of order k and which converges uniformly in γ and s for s in any finite interval (see [5], p. 368), and from (1), we obtain

$$\hat{Y}_{nm}(\epsilon, \delta, x) = i^n (2\pi)^{k/2} \left[\int_{\epsilon r}^{\delta r} J_{n+\lambda}(s)/s^{1+\lambda}\, ds \right] Y_{nm}(x').$$

Letting ϵ tend to zero and δ tend to infinity and on account of the formula (see [5], p. 391)

$$(12) \qquad \int_0^{\infty} J_{n+\lambda}(s)/s^{1+\lambda}\, ds = 2^{-\frac{1}{2}k}\Gamma(\tfrac{1}{2}n)/\Gamma(\tfrac{1}{2}[n+k]),$$

we obtain

$$(13) \qquad \hat{Y}_{nm}(x) = i^n \pi^{\frac{1}{2}k}\Gamma(\tfrac{1}{2}n)/\Gamma(\tfrac{1}{2}[k+n])\, Y_{nm}(x').$$

In the case $k = 2$, we write $y_1 = \rho\cos\phi$, $y_2 = \rho\sin\phi$, $x_1 = r\cos\theta$, $x_2 = r\sin\theta$, and the inner integral on the right-hand side of (10) becomes

$$\int_0^{2\pi} e^{is\cos(\phi-\theta)} \cos n(\phi - \phi_0)\, d\phi = 2\pi J_n(s) i^n \cos n(\theta - \phi_0),$$

and integrating and applying (12) we obtain (13).

4. In this section we shall consider the Riesz transforms and the operator Λ.

The Riesz transforms are defined as follows. Let

$$(14) \qquad R_{m\epsilon}(f) = - i\pi^{-\frac{1}{2}(k+1)}\Gamma[\tfrac{1}{2}(k+1)] \int_{\epsilon<|x-y|} (x_m - y_m)/|x-y|^{k+1} f(y)\, dy.$$

Then

$$(15) \qquad R_m(f) = \operatorname*{l.i.m.}_{\epsilon\to 0} R_{m\epsilon}(f).$$

THEOREM 1. *If $f \in L^p$, $1 < p < \infty$, the limit on the right of* (15) *exists as a limit in the mean of order p, and*

$$(16) \qquad \| R_{m\epsilon} f \|_p \leqq A_p \| f \|_p,$$

where A_p depends only on p and k, and $\| f \|_p$ is the L^p-norm of f. If $f \in L_r{}^p$, $r \geqq 1$, then $R_m f \in L_r{}^p$

$$(\partial/\partial x_n)R_m = R_m(\partial/\partial x_n), \tag{17}$$

$$R_m(\partial/\partial x_n) = R_n(\partial/\partial x_m), \tag{18}$$

where $\partial/\partial x_n$ *is the operator differentiation with respect to* x_n.

Finally, R_m *is selfadjoint in the sense that if* $f \in L^p$ *and* $g \in L^q$, $1 < p < \infty$, $p^{-1} + q^{-1} = 1$, *then* $(R_m f, g) = (f, R_m g)$, *and*

$$\sum_{m=1}^{k} R_m^2 = I, \qquad R_m R_n = R_n R_m, \tag{19}$$

where I *is the identity operator.*

In order to establish these results it will be convenient to prove first the following

LEMMA 1. *Let* $f \in L_r^p$, *then there exists a sequence of functions* f_n *in* C^∞, *each vanishing outside a bounded set, such that* $\| f_n - f \|_p \to 0$ *and* $\| D_j f_n - D_j f \|_p \to 0$ *for each derivative* $D_j f$ *of* f *of order* $j \leqq r$.

Let $\phi(x)$ and $\psi(x)$ be two functions in C^∞ vanishing outside a bounded set. Assume that $\phi(x) = 1$ in a neighborhood of $x = 0$ and that

$$\int_{E_k} \psi(x)\,dx = 1.$$

Let $\phi_n = \phi(x/n)$ and $\psi_n = n^k \psi(nx)$. Then, if $\psi_n * f$ denotes the convolution of ψ_n and f, we have that

$$\| \psi_n * f - f \|_p \to 0 \tag{20}$$

and

$$\| \psi_n * D_j f - D_j f \|_p \to 0$$

as $n \to \infty$. Now, since ψ_n is in C^∞ and vanishes outside a bounded set, from the definition of derivatives of functions in L_r^p (see Section 2) and by differentiation under the integral sign, we obtain that

$$D_j(\psi_n * f) = (D_j \psi_n) * f = \psi_n * D_j f.$$

Consequently,

$$\| D_j(\psi_n * f) - D_j f \|_p \to 0. \tag{21}$$

Now since $\phi_n(x) \to 1$ for each x, and since each derivative of $\phi_n(x)$ converges uniformly to zero as $n \to \infty$, we have that

$$\begin{aligned} &\| D_j[\phi_n(\psi_n * f)] - \phi_n D_j(\psi_n * f) \|_p \to 0 \\ &\| \phi_n D_j(\psi_n * f) - D_j(\psi_n * f) \|_p \to 0. \end{aligned} \tag{22}$$

If we set now $f_n = \phi_n(\psi_n * f)$, the desired result follows from (20), (21) and (22).

We revert now to the proof of Theorem 1. If $f \in L^2$ the fact that $R_{m\epsilon}(f)$ converges in the mean of order 2 follows by taking Fourier transforms in (14). In the previous section, we showed that the Fourier transform of the kernel of the integral operator (14)[2] converges boundedly to $x_m |x|^{-1}$ as $\epsilon \to 0$, and this clearly implies the convergence of $R_{m\epsilon}(f)$ and (16).

In the general case, the convergence in the mean of $R_{m\epsilon}(f)$ and (16) follows from Theorem 1 in [3] (see also the remark on page 306 of the same paper).

In order to show that $R_m(f)$ belongs to L_r^p if f does, it will be sufficient to consider the case $r = 1$; the general case will follow from (17).

Let $f \in L_1^p$ and let f_n be a sequence of functions as in the preceding lemma. Then by differentiating under the integral sign, we obtain

$$(\partial/\partial x_l) R_{m\epsilon} f_n = R_{m\epsilon}(\partial/\partial x_l) f_n,$$

and, if g is in C^∞ and vanishes outside a bounded set,

$$(g, R_{m\epsilon}(\partial/\partial x_l) f_n) = (g, (\partial/\partial x_l) R_{m\epsilon} f_n) = -((\partial/\partial x_l) g, R_{m\epsilon} f_n)$$

and letting first ϵ tend to zero and then n tend to infinity, on account of (16) we obtain

$$(g, R_m(\partial/\partial x_l) f) = -((\partial/\partial x_l) g, R_m f),$$

which shows that $R_m f \in L_1^p$ and that (17) holds.

In order to establish (18), we observe that, for every g in C^∞ vanishing outside a bounded set, we have $R_m \partial g/\partial x_l = R_l \partial g/\partial x_m$ (as one readily sees by taking Fourier transforms), and replacing g by the f_n of Lemma 1 and passing to the limit, we obtain $R_m \partial f/\partial x_n = R_n \partial f/\partial x_m$ for every f in L_r^p, $r \geqq 1$.

Finally, if f and g are bounded and vanish outside a bounded set, we have $(R_m f, g) = (f, R_m g)$ by interchanging the order of integration, and

$$\sum_{m=1}^{k} R_m^2(f) = f, \qquad R_m R_n(f) = R_n R_m(f)$$

by taking Fourier transforms, whence the general case follows from the continuity of R_m in L^p, $1 < p < \infty$.

Definition 1. Let $f \in L_r^p$, $r \geqq 1$, $1 < p < \infty$. Then

$$\Lambda f = i \sum_1^k R_m \partial f/\partial x_m = i \sum_1^k (\partial/\partial x_m) R_m f.$$

---

[2] Observe that this kernel coincides, except for a numerical factor, with one of the functions $Y_{1,m}(\epsilon, x)$ in (9).

COROLLARY. *If* $f \in L_r^p$, $r \geqq 1$ *then* $\Lambda f \in L_{r-1}^p$ *and*

$$i\partial f/\partial x_n = R_n \Lambda f = \Lambda R_n f. \tag{23}$$

If $f \in L_r^p$, $r \geqq 2$ *then*

$$\Delta f = \sum_1^k \partial^2 f/dx_m{}^2 = -\Lambda^2 f. \tag{24}$$

The first assertion follows from the definition of Λ and the fact that the operators R_m preserve the classes L_r^p. The formulas (23) and (24) are obtained from the definition of Λ by using (18) and (19).

5. We proceed to present the main results of the paper. We begin with

THEOREM 2. *Let* $h(x,z)$, $x, z \in E_k$, *be a function in* C_β^∞, $\beta \geqq 0$, *homogeneous of degree* $-k$ *in* z, *that is, such that* $h(x, \lambda z) = \lambda^{-k} h(x,z)$ *for every* $\lambda > 0$, *and assume that* $\int_\Sigma h(x,z)\,d\sigma = 0$ *for every* x, *where* Σ *is the sphere* $|z| = 1$. *Let* $a(x)$ *be a function in* C_β, *and consider the operator*

$$H_\epsilon f = a(x) f(x) + \int_{|x-y|>\epsilon} h(x, x-y) f(y)\,dy \tag{25}$$

and its adjoint

$$H_\epsilon^* f = \bar{a}(x) f(x) + \int_{|x-y|>\epsilon} \bar{h}(y, y-x) f(y)\,dy. \tag{26}$$

Then

i) H_ϵ *and* H_ϵ^* *are defined for* $f \in L^p$, $1 < p < \infty$ *and as* $\epsilon \to 0$, $H_\epsilon(f)$ *and* $H_\epsilon^*(f)$ *converge in the mean of order* p. *If* $H(f)$ *and* $H^*(f)$ *denote their respective limits, we have*

$$\begin{aligned} \| Hf \|_p &\leqq \| f \|_p A_p \sup_{|z|=1} (|a(x)| + |h(x,z)|), \\ \| H^* f \|_p &\leqq \| f \|_p A_q \sup_{|z|=1} (|a(x)| + |h(x,z)|), \end{aligned} \tag{27}$$

where $p^{-1} + q^{-1} = 1$ *and* A_p *depends only on* p *and* k.

ii) *if* $f \in L_r^p$, $1 < p < \infty$, *with* $r \leqq \beta$, *then* Hf *and* $H^* f$ *belong to* L_r^p,

iii) *if* $f \in L^p$, $1 < p < \infty$, *and is Hölder-continuous of order* α, $0 < \alpha < \beta$, Hf *and* $H^* f$ *are Hölder continuous of the same order.*

Part of i) concerning the operators H_ϵ and H was proved in [3], Theorem 2. The estimate of $\| Hf \|_p$, which also holds for $\| H_\epsilon f \|_p$, is not given explicitly there but is contained in the proof of the theorem. We shall therefore concentrate in the case $p = 2$. We begin with

LEMMA 2. *Let*

$$T_{nm\epsilon}f = \int_{|x-y|>\epsilon} Y_{nm}(\epsilon, x-y) f(y)\, dy, \tag{28}$$

where $Y_{nm}(\epsilon, x)$ *is the function defined in* (9). *Then if* $f \in L^p$, $1 < p < \infty$, *there is a constant* A_p *depending on* p *and* k *such that*

$$\| T_{nm\epsilon} f \|_p \leqq A_p \| f \|_p, \tag{29}$$

and as $\epsilon \rightarrow 0$, $T_{nm\epsilon}f$ *converges in the mean of order* p *to a limit* $T_{nm}f$. *If* $f \in L_r^p$, *then* $T_{nm}f \in L_r^p$. *The operators* T_{nm} *commute with the* R_m *of Theorem* 1 *and when acting on* L_r^p, *they also commute with the* $\partial/\partial x_n$.

The proof of this lemma proceeds as that of Theorem 1 and we need not repeat it here.

Now we revert to the operator H_ϵ. Let us expand the function $h(x, z)$ in spherical harmonics

$$h(x, z) = \Sigma a_{nm}(x) Y_{nm}(z') \, | z |^{-k}, \tag{31}$$

where the $a_{nm}(x)$ can be calculated by means of formula (8) after replacing F by h. Since, for each n, the number of distinct spherical harmonics Y_{nm} is of the order n^{k-2} and since, according to (3), Y_{nm} has a bound of the order $n^{\frac{1}{2}(k-2)}$, it follows from the formula (8), by choosing r sufficiently large, that the series of absolute values of the terms of the series above is dominated by a multiple of $| z |^{-k}$. Consequently, given $f \in L^p$, we can replace h by the series in (25) and (26) and integrate term by term obtaining

$$H_\epsilon f = a(x) f + \Sigma a_{nm}(x) T_{nm\epsilon} f, \qquad H_\epsilon^* f = \bar{a}(x) f + \Sigma (-1)^n T_{nm\epsilon}(\bar{a}_{nm} f). \tag{32}$$

Now the $a_{nm}(x)$ are dominated in absolute value by the terms of a convergent numerical series, and according to (29), the $T_{nm\epsilon}f$ are bounded in norm and converge in the mean as $\epsilon \rightarrow 0$. Hence $H_\epsilon f$ converges in the mean. Similarly, the functions $T_{nm\epsilon}(\bar{a}_{nm} f)$ converge in the mean and their norms are dominated by the terms of a convergent numerical series, which implies that $H_\epsilon^* f$ also converges.

Passing to the limit we obtain

$$Hf = a(x) f + \Sigma a_{nm}(x) T_{nm} f, \qquad H^* f = \bar{a}(x) f + \Sigma (-1)^n T_{nm}(\bar{a}_{nm} f), \tag{33}$$

the series converging in the mean of order p. If f and g vanish outside a bounded set and are bounded, from absolute integrability, it follows that $(H_\epsilon f, g) = (f, H_\epsilon^* g)$ and from the continuity of the operators H_ϵ and H_ϵ^* in every L^p, $1 < p < \infty$, we obtain $(H_\epsilon f, g) = (f, H_\epsilon^* g)$ for $f \in L^p$ and $g \in L^q$, $p^{-1} + q^{-1} = 1$, which justifies the assertion that H_ϵ^* is the adjoint of H_ϵ.

By a passage to the limit we obtain that also H^* is the adjoint of H.

Our next step will be establishing (27) in the case $p=2$. In the first place, we have that

$$|a(x)|^2+\Sigma\,|a_{nm}(x)|^2 \leqq \sup_x\,[\,|a(x)|^2+\int_{|z|=1}|h(x,z)|^2\,d\sigma]=C^2,$$

and from (33) and Schwarz's inequality, we obtain

$$|Hf|^2 \leqq C^2[\,|f|^2+\Sigma\,|T_{nm}f|^2].$$

Integrating and applying Plancherel's theorem to the right hand side, we obtain (see formula (13))

$$\|Hf\|_2{}^2 \leqq C^2\int_{E_k}[1+\Sigma\pi^k\{\Gamma(\tfrac{1}{2}n)/\Gamma(\tfrac{1}{2}[k+n])\}^2 Y_{nm}(x')^2]\,|\hat{f}(x)|^2\,dx.$$

Now the sum of the squares of the spherical harmonics of a given degree n is a constant equal to the number of such harmonics divided by the area of Σ (see [1], p. 242). Since this number is of the order n^{k-2}, the series in the last integral is absolutely convergent and represents a constant, and we obtain

$$\|H_f\|_2{}^2 \leqq C^2A_2{}^2\,\|f\|_2{}^2=C^2A_2{}^2\,\|f\|_2{}^2,$$

where $A_2{}^2$ is the value of the series, which is the first inequality in (27). The second is obtained from the fact that H^* is the adjoint of H.

We turn now to the proof of ii). Since the $a_{nm}(x)$ can be calculated by means of formula (8), replacing the function F there by $h(x,z)$, it follows readily by choosing r sufficiently large, that the $a_{nm}(x)$ and their derivatives of order less than or equal to β are dominated in absolute value by the terms of a convergent numerical series. Now if $f\in L_r{}^p$, then $T_{nm}f$ and $T_{nm}(a_{nm}f)$ belong to $L_r{}^p$, and from (29) it follows that the series in (33) can be differentiated term by term, which establishes ii).

In order to establish iii), we shall first investigate the Hölder continuity of $T_{nm}f$. Write $h(x)=Y_{nm}(x')\,|x|^{-k}$ and let S be any set contained in a sphere of radius ρ with center at x. Then if $f(x)$ is Hölder continuous of order α, $0<\alpha<1$, and $|f(x_1)-f(x_2)|\leqq A\,|x_1-x_2|^\alpha$, inequality (3) gives

$$(34)\qquad \left|\int_S h(x-y)[f(y)-f(x)]\,dy\right| \leqq \int_{|x-y|\leqq\rho} CAn^{\frac{1}{2}(k-2)}\,|x-y|^{-k+\alpha}\,dy = C/\alpha\,An^{\frac{1}{2}(k-2)}\rho^\alpha.$$

In particular, we have

$$(35)\qquad \left|\int_{|x-y|\leqq\rho} h(x-y)f(y)\,dy\right| \leqq \left|\int_{|x-y|\leqq\rho} h(x-y)[f(y)-f(x)]\,dy\right| \leqq C/\alpha\,An^{\frac{1}{2}(k-2)}\rho^\alpha.$$

Let now x_1 and x_2 be two points. Set $\rho = 2\,|\,x_1 - x_2\,|$ and write

$$(T_{nm}f)(x_1) - (T_{nm}f)(x_2)$$
$$= \int_{|x_1-y|\leqq\rho} h(x_1-y)f(y)\,dy + \int_{|x_1-y|\geqq\rho} h(x_1-y)[f(y)-f(x_2)]\,dy$$
$$- \int_{|x_1-y|\leqq\rho} h(x_2-y)[f(y)-f(x_2)]\,dy + \int_{|x_1-y|\geqq\rho} h(x_2-y)[f(y)-f(x_2)]\,dy,$$

where the integrals over $|\,y-x_1\,| \geqq \rho$ are understood as the limit as $R \to \infty$ of the integrals extended over $\rho \leqq |\,y-x_1\,| \leqq R$. Then from (34) and (25), we obtain

$$|\,(T_{nm}f)(x_1) - (T_{nm}f)(x_2)\,| \leqq C/\alpha\, An^{\frac{1}{2}(k-2)}\rho^{\alpha}$$
$$+ \int_{|x_1-y|\geqq\rho} |\,h(x_1-h) - h(x_2-y)\,|\,|\,f(y)-f(x_2)\,|\,dy.$$

Now according to (4), $|\,h(x_1-y) - h(x_2-y)\,| \leqq Cn^{k/2}\,|\,x_1-x_2\,|\,|\,x_1-y\,|^{-k-1}$ in $|\,x_1-y\,| \geqq \rho$, and since $|\,f(y)-f(x_2)\,| \leqq A\,|\,y-x_2\,|^{\alpha}$ and $|\,y-x_2\,| \leqq 2\,|\,y-x_1\,|$ in $|\,x_1-y\,| \geqq \rho$, it follows that

$$\begin{aligned} &|\,(T_{nm}f)(x_1) - (T_{nm}f)(x_2)\,| \leqq C/\alpha\, An^{\frac{1}{2}(k-2)}\rho^{\alpha} \\ &+ CAn^{k/2}\,|\,x_1-x_2\,| \int_{\rho}^{\infty} s^{\alpha-2}\,ds \leqq [1/\alpha + 1/(1-\alpha)]CAn^{k/2}\,|x_1-x_2\,|^{\alpha}, \end{aligned} \tag{36}$$

where the constant C in the last expression depends only on k. Further, since $\|\,T_{nm}f\,\|_p$ is bounded, as is readily verified, (36) implies that $(T_{nm}f)(x)$ has a bound of the order $n^{k/2}$. Now we can estimate $(Hf)(x_1) - (Hf)(x_2)$ from the series in (33). To obtain the desired result, it suffices to observe that, for every r, the functions $a_{nm}(x)n^r$ are uniformly bounded and uniformly Hölder continuous. This follows from formula (8) and allows us to estimate the preceding difference by estimating the corresponding differences of the terms of the series. The Hölder continuity of H^*f is established by a similar argument.

Remark. Infinite differentiability of $h(x, z)$ with respect to z is not indispensable for the validity of the preceding theorem, and, indeed, the argument used in its proof remains valid under weaker assumptions.

Another fact worth mentioning is this. Not only do the functions $H_\epsilon f$ and $H_\epsilon{}^*f$ converge in the mean of order p if f is in L^p, $1 < p < \infty$, but they converge pointwise almost everywhere and are dominated in absolute value by functions in L^p. For $H_\epsilon f$, this result is contained in Theorem 2 of [3]. The result for $H_\epsilon{}^*f$ can be obtained by applying Theorem 1 in [3] [3] to each of the terms of the expansion in (33) after observing that the $a_{nm}(x)$ are dominated in absolute value by the terms of a convergent numerical series.

---

[3] See also the remark on page 306 of the same paper.

Definition 2. A singular integral operator of type C_β^∞ is an operator such as the H of Theorem 2. The symbol of the operator H is the function

$$\sigma(H) = a(x) + \Sigma a_{nm}(x)\gamma_n Y_{nm}(z'), \tag{37}$$

where $a(x)$ is the function in (25), *the $a_{nm}(x)$ are the functions in* (31), *and*

$$\gamma_n = i^n \pi^{k/2}\Gamma(\tfrac{1}{2}n)/\Gamma(\tfrac{1}{2}[n+k]). \tag{38}$$

The reader will notice that, on account of (13) the summation sign in (37) represents in a sense the Fourier transform of $h(x, z)$ with respect to z. This fact could be used in defining the symbol $\sigma(H)$ of H, but in the present set-up we find the preceding definition more convenient.

THEOREM 3. *If H is a singular integral operator of type C_β^∞ its symbol is a homogeneous function of degree zero with respect to z and in C_β^∞ in $|z| \geqq 1$. Conversely, every function of x and z which is homogeneous of degree zero with respect to z and belongs to C_β^∞ in $|z| \geqq 1$ is the symbol of a unique operator of type C_β^∞. If M is a bound for the absolute value of $\sigma(H)$ and its derivatives with respect to the coordinates of z in $|z| \geqq 1$ of order $2k$, then*

$$\| Hf \|_p \leqq MA_p \| f \|_p \tag{39}$$

where A_p depends only on p and k.

According to formula (8), we have

$$\begin{aligned} a_{nm}(x) &= (-1)^r n^{-r}(n+k-2)^{-r} \int_\Sigma L^r[h(x, z')] Y_{nm}(z') d\sigma, \\ a_{nm}(x) &= (-1)^r \gamma_n^{-1} n^{-r}(n+k-2)^{-r} \int_\Sigma L^r[\sigma(H)(x, z')] Y_{nm}(z') d\sigma, \end{aligned} \tag{40}$$

where L is the operator defined in (5) and x is regarded as a parameter. From this representation it follows readily that, if $h(x, z)$ or $\sigma(H)(x, z)$ belongs to C_β^∞ in $|z| \geqq 1$, then, for each r, the functions $a_{nm}(x)n^r$ are uniformly in C_β. Conversely, if the latter holds, by taking (4) into account and differentiating the series (31) and (37) term by term, we obtain that both $h(x, z)$ and $\sigma(H)(x, z)$ belong to C_β^∞ in $|z| \geqq 1$.

In order to establish (39) we just set $r = k$ in the last formula and obtain $|a_{nm}(x)| \leqq CMn^{-\frac{3}{2}k}$ where C is a constant depending only on k.

This combined with (3), (31) and the fact that the number of distinct spherical harmonics of degree n is of the order n^{k-2} yields $|h(x,z)| \leqq CM$, where again C depends only on k. But on account of (27), this implies (39).

Definition 3. Let H, H_1 and H_2 be singular integral operators of type C_β^∞. We define $H^\#$ and $H_1 \circ H_2$ by the formulas

$$\sigma(H^\#) = \bar{\sigma}(H), \qquad \sigma(H_1 \circ H_2) = \sigma(H_1)\sigma(H_2),$$

where $\bar{\sigma}(H)$ is the complex conjugate of $\sigma(H)$.

THEOREM 4. *If the symbols of H, H_1 and H_2 are independent of x, then $H^\# = H^*$, $H_1 \circ H_2 = H_1 H_2 = H_2 H_1$ where $H_1 H_2$ is the composition product of H_1 and H_2.*

Let $f(x)$ be bounded and vanish outside a bounded set and let $\hat{f}$ be its Fourier transform. Then according to (32), we have $H_\epsilon f = af + \Sigma a_{nm} T_{nm\epsilon} f$, where a and a_{nm} are the same as those in (37) and are therefore assumed to be independent of x. Taking Fourier transforms and letting ϵ tend to zero, we obtain on account of (13)

$$(Hf)^\wedge = a\hat{f}(z) + \Sigma a_{nm}\gamma_n Y_{nm}(z')\hat{f}(z);$$

that is, $(Hf)^\wedge = \sigma(H)\hat{f}$, whence

$$(H^*f)^\wedge = \bar{\sigma}(H)\hat{f} = (H^\# f)^\wedge, \qquad [(H_1 \circ H_2)f]^\wedge = \sigma(H_1)\sigma(H_2)\hat{f} = (H_1 H_2 f)^\wedge.$$

which implies that $H^*f = H^\# f$ and $(H_1 \circ H_2)f = H_1 H_2 f$. From this and the continuity of H in L^p, the desired result follows.

COROLLARY. *If the symbol of the singular integral operator H is independent of x and does not vanish, then H has an inverse and the inverse is also a singular integral operator.*

Clearly the operator H_1 defined by $\sigma(H_1) = \sigma(H)^{-1}$ is an inverse of H.

The following theorem deals with the relationship between H^* and $H^\#$, and $H_1 H_2$ and $H_1 \circ H_2$ in the general case.

THEOREM 5. *Let H be an operator of type C_β^∞ with $\beta > 1$. Let M be a bound for $\sigma(H)(x,z)$ and its derivatives with respect to coordinates of z of order $2k$, the first derivatives of these with respect to the coordinates of x, and the Hölder constants of the latter. Then for every $f \in L_1^p$, $1 < p < \infty$, we have*

$$(41) \qquad \begin{aligned} &\|(H\Lambda - \Lambda H)f\|_p \leqq A_p M \|f\|_p, \quad \|(H^*\Lambda - \Lambda H^*)f\|_p \leqq A_p M \|f\|_p, \\ &\|(H^* - H^\#)\Lambda f\|_p \leqq A_p M \|f\|_p, \quad \|\Lambda(H^* - H^\#)f\|_p \leqq A_p M \|f\|_p, \end{aligned}$$

where A_p *depends only on* p, k *and* β. *Further, if* H_1 *and* H_2 *are two operators in* C_β^∞ *and* $f \in L_1^p$ *then*

$$\begin{aligned} &\| (H_1 \circ H_2 - H_1H_2)\Lambda f \|_p \leqq A_p M_1 M_2 \| f \|_p, \\ (42) \qquad & \\ &\| \Lambda(H_1 \circ H_2 - H_1H_2) f \|_p \leqq A_p M_1 M_2 \| f \|_p, \end{aligned}$$

where, again, A_p *depends only on* p, k *and* β *and* M_1 *and* M_2 *are defined as above.*

Let $c(x)$ be a function in C_β, T a singular integral operator with symbol independent of x, and f a function in C^∞ and vanishing outside a a bounded set. Denote by $Y(z)$ the kernel of the operator T, and consider the expression

$$(43) \qquad (cT - Tc)f_{x_i} = \lim_{\epsilon \to 0} \int_{|x-y|>\epsilon} [c(x) - c(y)] Y(x-y) f_{y_i}\, dy,$$

where f_{x_i} stands for $\partial f/\partial x_i$. Since $c(x) \in C_\beta$, $\beta > 1$, if $0 < \alpha \leqq \beta - [\beta]$, and $\alpha \leqq 1$, we have

$$| c_{x_j}(x) - c_{x_j}(y) | \leqq A \, | x - y |^\alpha,$$
$$c(x) - c(y) = \sum_j (x_j - y_j) c_{x_j}(x) + b(x,y),$$

where $| b(x,y) | \leqq kA \, | x - y |^{1+\alpha}$. Now we replace this expression in the integral in (43) and integrate by parts, obtaining

$$\begin{aligned} & \int_{|x-y|>\epsilon} Y(x-y) c_{x_i}(y) f(y)\, dy \\ & + \int_{\epsilon<|x-y|\leqq 1} \sum_j (x_j - y_j) c_{x_j}(x) Y_{x_i}(x-y) f(y)\, dy \\ (44) \qquad & + \int_{|x-y|>1} [c(x) - c(y)] Y_{x_i}(x-y) f(y)\, dy \\ & + \int_{\epsilon<|x-y|\leqq 1} b(x,y) Y_{x_i}(x-y) f(y)\, dy \\ & + \int_{|x-y|=\epsilon} [c(x) - c(y)] Y(x-y) f(y) \gamma_i\, d\sigma, \end{aligned}$$

where the last integral is extended over the surface of the sphere $| x - y | = \epsilon$ and γ_i is the i-th direction cosine of the normal to the spherical surface. Denote now by N_1 a bound for $| c(x) |$, $| c_{x_j} |$ and the Hölder constants for the derivatives c_{x_j}, and by N_2 a bound for $| Y(z) |$ and $| Y_{z_i}(z) |$ on $| z | = 1$, and observe that the functions $z_j Y_{z_i}(z)$, are homogeneous of degree $-k$ and their mean value over the sphere $| z | = 1$ is zero (otherwise, if $f(x) \neq 0$ and $c_{x_n} = \delta_{nj}$, the second integral in (44) would diverge as ϵ tends to zero while the remaining terms and the whole expression converge). Thus if we let ϵ

tend to zero in (44) and apply Theorem 1 in [3] (see also the remark on page 306 of the same paper) to the first two terms, we see that they represent a function of x whose L^p-norm does not exceed $AN_1N_2 \, \| f \|_p$ where A depends only on p and k. In the case $f \in L^2$, we apply Theorem 2 to the first term. The second term is not suitable for a direct application of Theorem 2, but the convolution integrals

$$\int_{\epsilon<|x-y|\leqq 1} (x_j - y_j) Y_{x_l}(x-y) f(y) \, dy$$

can be easily estimated by taking Fourier transforms and estimating the transform of $z_j Y_{x_l}(z)$ multiplied by the characteristic function of $\epsilon < |z| \leqq 1$ using the method used in Section 3.

Since $Y_{z_l}(z)$ is homogeneous of degree $-k-1$, it is absolutely integrable over $|z| \geqq 1$, and, on account of the estimate for $b(x,y)$, one sees readily that the third and fourth terms in (44) are dominated by convolutions of $|f(y)|$ with absolutely integrable functions. Hence, it follows from a theorem of Young that they represent functions whose L^p-norms are less than or equal to $\| f \|_p$ times the L^1-norms of those integrable functions, and an easy computation yields $AN_1N_2 \, \| f \|_p$ as a bound for the L^p-norms of those functions, where the constant A depends on k and α. Finally, one sees readily that, as ϵ tends to zero, the last term in (44) tends to a limit whose absolute value is dominated by $AN_1N_2 \, |f(x)|$, where A depends only on k. Collecting results and applying Lemma 1, we obtain

$$\| (cT - Tc) f_{x_l} \|_p \leqq A_p N_1 N_2 \, \| f \|_p, \tag{45}$$

for every f in L_1^p, $1 < p < \infty$, where A_p depends only on p, k and α (or β). Having established (45), we can proceed to prove the inequalities (41) and (42).

Consider the representation of Hf and H^*f given in (33). Write $a_0(x)$ for $a(x)$ and T_0 for the identity operator. Then since the $a_{nm}(x)$ are dominated in absolute value by a convergent numerical series and since the T_{nm} as operators on L^p, $1 < p < \infty$, have bounded norm for each fixed p, we may write

$$H = \sum_{n\geqq 0} a_{nm} T_{nm}, \qquad H^* = \sum_{n\geqq 0} (-1)^n T_{nm} \bar{a}_{nm}, \qquad H^\# = \sum_{n\geqq 0} (-1)^n \bar{a}_{nm} T_{nm},$$

where the series on the right converge in the operator norm. If f is in L_1^p, then

$$\begin{aligned}(\Lambda H - H\Lambda) f &= \sum_{l=1}^{k} R_l \left(\sum a_{nm} T_{nm} f\right)_{x_l} - \sum a_{nm} T_{nm} \left(\sum R_l f_{x_l}\right) \\ &= \sum_{l,n} R_l (a_{nm})_{x_l} T_{nm} f + \sum_{l,n} (R_l a_{nm} - a_{nm} R_l)(T_{nm} f)_{x_l}\end{aligned}$$

since the $(a_{nm})_{x_l}$ are dominated by a convergent numerical series which justifies term by term differentiation of the first series above. Now we apply (45) to each of the terms of the last series, estimating N_1 each time from the second formula in (40), and use (29) obtaining readily the first inequality in (41). The second inequality in (41) follows by an argument almost identical to the preceding one. In order to prove the third inequality in (41), we write

$$\begin{aligned}(H^*-H^\#)\Lambda f &= \sum_{l=1}^{k}(H^*-H^\#)(R_lf)_{x_l}\\ &= \sum_{l,n}(-1)^n(T_{nm}\bar{a}_{nm}-\bar{a}_{nm}T_{nm})(R_lf)_{x_l},\end{aligned}$$

and again (45) combined with (40) and (4) yields the desired result.

The last inequality in (41) is readily seen to be an immediate consequence of the preceding ones.

Let now $H_1=\sum b_{nm}T_{nm}$, $H_2=\sum c_{nm}T_{nm}$, and consider the series of operators

$$\sum b_{nm}c_{\nu\mu}T_{nm}T_{\nu\mu}, \tag{46}$$

the sum being extended over all indices, and the series of their symbols

$$\begin{aligned}&\sum b_{nm}(x)c_{\nu\mu}(x)Y_{nm}(z')Y_{\nu\mu}(z')\gamma_n\gamma_\nu\\ &=(\sum b_{nm}(x)Y_{nm}(z')\gamma_n)(\sum c_{\nu\mu}(x)Y_{\nu\mu}(z')\gamma_\nu)=\sigma(H_1)\sigma(H_2)=\sigma(H_1\circ H_2).\end{aligned} \tag{47}$$

From the estimate (4) of the successive derivatives of $Y_n(z')$ and the formula (40) applied to the coefficients b_{nm} and $c_{\nu\mu}$, it follows that the first series in (47) converges uniformly as well as the series obtained from it by differentiating its terms with respect to coordinates of z any number of times. But then Theorem 3 implies that (46) converges in the operator norm and that (47) is precisely the symbol of (46), or, equivalently, that (46) is precisely $H_1\circ H_2$. On the other hand, since the functions $b_{nm}(x)$ and $c_{nm}(x)$ are dominated by convergent numerical series we have

$$H_1H_2=\sum b_{nm}T_{nm}c_{\nu\mu}T_{\nu\mu},\qquad H_1\circ H_2-H_1H_2=\sum b_{nm}(c_{\nu\mu}T_{nm}-T_{nm}c_{\nu\mu})T_{\nu\mu}.$$

Thus

$$\begin{aligned}(H_1\circ H_2-H_1H_2)\Lambda f &= \sum b_{nm}(c_{\nu\mu}T_{nm}-T_{nm}c_{\nu\mu})T_{\nu\mu}(R_lf)_{x_l}\\ &= \sum b_{nm}(c_{\nu\mu}T_{nm}-T_{nm}c_{\nu\mu})(T_{\nu\mu}R_lf)_{x_l}.\end{aligned}$$

If we now compute the $c_{\nu\mu}$ and b_{nm} by means of (40) and apply (45) using (3) and (4) in order to estimate the kernel of T_{nm} and its first order derivatives, and bear in mind that the $T_{\nu\mu}$ are uniformly bounded in L^p and that, for each n, the number of distinct T_{nm} is of the order n^{k-2}, we obtain the first inequality in (42). The second follows immediately from the first and the first inequality in (41). Theorem 5 is thus established.

THEOREM 6. *Let* $\mathfrak{A}_p$ *be the algebra of bounded operators on* L^p, $1 < p < \infty$ *generated by all singular integral operators* H *of type* C_β^∞, $\beta > 1$, *and their adjoints* H^* *(see definition 2 and Theorem 2). Then there exists a homomorphism* h_p *of* $\mathfrak{A}_p$ *onto the algebra of all functions* $F(x,z)$ *in* C_β^∞ *which are homogeneous of degree zero with respect to* z, *such that, for every singular integral operator* H, *the identities* $h_p(H) = \sigma(H)$, $h_p(H^*) = \bar{\sigma}(H)$ *hold. The kernel of* h_p *can be characterized as follows:* K *belongs to the kernel of* h_p, *or, equivalently,* $h_p(K) = 0$, *if and only if there exists a positive constant* A *depending on* K *such that* $\| K\Lambda f \|_p \leqq A \| f \|_p$ *for every* $f \in L_1^p$. *If* $h_p(K)$ *is bounded away from zero, then there exists* $K' \in \mathfrak{A}_p$ *with a two sided inverse, such that* $h_p(K) = h_p(K')$.

Every bounded operator on L^p *which commutes with every operator in* $\mathfrak{A}_p$ *is a multiple of the identity operator.*

The algebras $\mathfrak{A}_p$, $\mathfrak{A}_q$ *corresponding to any two spaces* L^p *and* L^q, $1 < p < q < \infty$, *are isomorphic and there is a natural isomorphism* ϕ *between* $\mathfrak{A}_p$ *and* $\mathfrak{A}_q$ *such that* $h_p = h_q\phi$.

We start with the following

LEMMA. *Let* H *be a singular integral operator of type* C_β^∞, $\beta > 1$. *Assume that for some positive constant* A *and every* $f \in L_1^p$ *the inequality* $\| H\Lambda f \|_p \leqq A \| f \|_p$ *holds. Then* $H = 0$.

Let $\mathfrak{G}$ be the class of functions which are symbols of singular integral operators with the property that $H\Lambda$ is bounded in the sense just described. Then $\mathfrak{G}$ is linear, and, on account of (42) and the definition 3, it is closed under multiplication by functions $F(x,z)$ in C_β^∞ which are homogeneous of degree zero with respect to z. Let u be a rotation of E_k about the point x_0. Then, if we denote $f[u(x)]$ by $f_u(x)$ and $\sigma(H)$ by $F(x,z)$, and define H_u and F_u by

$$F_u(x,z) = \sigma(H_u) = F[u(x), u(z+x_0) - x_0],$$

we have the following identities

$$\| f \|_p = \| f_u \|_p, \qquad (\Lambda f)_u = \Lambda f_u, \qquad (Hf)_u = H_u f_u.$$

Consequently, if $F(x,z) \in \mathfrak{G}$ then

$$\| H_u \Lambda f_u \|_p = \| H_u(\Lambda f)_u \|_p = \| (H\Lambda f)_u \|_p = \| H\Lambda f \|_p \leqq A \| f \|_p = A \| f_u \|_p$$

which shows that $F_u \in \mathfrak{G}$. Assume now that $F(x_0, z)$ is not identically zero in z. Then there exist finitely many rotations u_i of E_k about x_0 such that

$G(x,z)=\Sigma\,|F_{u_i}(x,z)|^2$ has the property that $G(x_0,z)$ does not vanish. Let now $a(x)$ be a function in C_β such that $a(x_0)\neq 0$ and vanishing outside a neighborhood of x_0 where $G(x,z)$ is bounded away from zero, and define $G_1(x,z)=a(x)G(x,z)^{-1}$, where $a(x)\neq 0$, and $G_1(x,z)=0$ otherwise. Then $G_1Gz_1\,|z|^{-1}=a(x)z_1\,|z|^{-1}$, and since $F_{u_i}\in\mathcal{B}$, it follows that $a(x)z_1\,|z|^{-1}\in\mathcal{B}$. Now $a(x)z_1\,|z|^{-1}$ is the symbol of the operator $a(x)R_1$ and therefore, on account of (23), we have that

$$\|a(x)R_1\Lambda f\|_p=\|ia(x)f_{x_1}\|_p\leqq A\,\|f\|_p$$

for every function f in $L_1{}^p$. But this is clearly impossible unless $a(x)=0$ identically which contradicts our assumptions. Hence we must have $F(x_0,z)=0$ for every z. Since the same argument applies to an arbitrary point x_0 we must have $F(x,z)=0$ identically, and the only function in $\mathcal{B}$ is zero. This establishes the lemma.

Now let us revert to the proof of Theorem 6. Consider the class $\mathcal{B}$ of opeartors K in $\mathfrak{A}_p$ with the property that there exists a singular integral operator H and a constant A such that $\|(K-H)\Lambda f\|_p\leqq A\,\|f\|_p$ for every $f\in L_1{}^p$. Then $\mathcal{B}$ is clearly linear. Further, it follows from (41) and (42) that $\mathcal{B}$ is closed under multiplication. Now every singular integral operator belongs to $\mathcal{B}$, and the third inequality in (41) implies that their adjoints also belong to $\mathcal{B}$; that is, $\mathcal{B}$ is an algebra containing all singular integral operators and their adjoints. Hence $\mathcal{B}$ coincides with $\mathfrak{A}_p$.

The singular integral operator H associated with K in the manner described above is unique, as follows immediately from the preceding lemma. Now we define $h_p(K)$ to be $\sigma(H)$. Then h_p is clearly linear and, on account of (41) and (42), multiplicative. Since the mapping $H\rightarrow\sigma(H)$ is onto the class of all functions $F(x,z)$ in $C_\beta{}^\infty$ which are homogeneous of degree zero with respect to z, the same applies to h_p. The identity $h_p(H)=\sigma(H)$ for every singular integral operator H is clear, and $h(H^*)=\bar{\sigma}(H)$ follows from the third inequality in (41). Further, the fact that $h_p(K)=0$ if and only if $K\Lambda$ is bounded in the sense described above is an immediate consequence of the definition of h_p.

Suppose now that $h_p(K)=F(x,z)$ is bounded away from zero. Let $z_0\neq 0$ be a fixed point in E_k and set

$$a(x)=F(x,z_0)F(0,z_0)^{-1},\qquad G(x,z)=F(x,z)a(x)^{-1}F(0,z)^{-1}.$$

Then $G(0,z)=G(x,z_0)=1$ and this, as is readily verified, implies that $G(x,z)$ has an n-th root $G(x,z)^{1/n}$ in $C_\beta{}^\infty$. If we choose $G(x,z)^{1/n}$ so that $G(0,z)^{1/n}=1$, the boundedness of the first order derivatives of $G(x,z)$ and the fact that $G(x,z_0)=1$ imply that $G(x,z)^{1/n}$ converges uniformly to 1 and its derivatives with respect to coordinates of z of order $2k$ converge uniformly to zero in $|z| \geqq 1$. Thus theorem (3) implies that, for n sufficiently large, the operator H defined by $\sigma(H) = G(x,z)^{1/n}$ is close to the identity operator, or, more precisely, $\| I - H \| < \frac{1}{2}$, where I is the identity and the norm is taken in the sense of operator norm. But this implies that H has a two sided inverse. Further, define H_1 and H_2 by $\sigma(H_2) = F(0,z)$ and $\sigma(H_1) = a(x)$. Then since $a(x)$ is bounded away from zero, H_1 has an inverse, and since $F(0,z)$ does not vanish, according to the Corollary to Theorem 4, H_2 also has an inverse. Define now $K' = H_1 H_2 H^n$. Then K' has an inverse and

$$\begin{aligned} h_p(K') &= h_p(H_1) h_p(H_2) h_p(H)^n \\ &= \sigma(H_1)\sigma(H_2)\sigma(H)^n = a(x)F(0,z)G(x,z) = F(x,z) = h_p(K) \end{aligned}$$

which establishes the corresponding statement in the Lemma.

Let now K be a bounded operator on L^p which commutes with all singular integral operators. In particular, K commutes with multiplication by functions in C_β, that is, if $a(x) \in C_\beta$ then $K(af) = aK(f)$ for every $f \in L^p$. Assume now that f is positive, continuous and in L^p and consider the function $\psi(x) = f^{-1}K(f)$. Then for every $g(x)$ of the form $g(x) = f(x)a(x)$ with $a(x) \in C_\beta$ we have $K(g) = K(af) = aK(f) = af[f^{-1}K(f)] = g(x)\psi(x)$. Since K is continuous on L^p and the functions of the form $a(x)f(x)$ are dense in L^p, it follows both that $\psi(x)$ is essentially bounded and that $K(g) = \psi g$ for every $g \in L^p$. Let now $\bar{x}$ be a point at which $\psi(x)$ is equal to the derivative of its indefinite integral and $f_n(x)$ a function which is constant on the sphere with center at $\bar{x}$ and radius $1/n$, vanishes outside this sphere and has integral equal to 1. If H is a singular integral operator with kernel $h(x-y)$, then

$$HKf_n = \lim_{\epsilon \to 0} \int_{|x-y|>\epsilon} h(x-y)\psi(y)f_n(y)\,dy$$

converges towards $h(x-\bar{x})\psi(\bar{x})$ for all x, $x \neq \bar{x}$. On the other hand,

$$KHf_n = \psi(x) \lim_{\epsilon \to 0} \int_{|x-y|>\epsilon} h(x-y)f_n(y)\,dy$$

converges towards $h(x-\bar{x})\psi(x)$. Since H and K commute we have $KHf_n = HKf_n$, and therefore $h(x-\bar{x})\psi(x) = h(x-\bar{x})\psi(\bar{x})$ almost everywhere. If we assume, as we may, that $h(x)$ does not vanish identically on a set of positive measure, it follows that $\psi(x) = \psi(\bar{x})$ almost everywhere, and this implies that K is a multiple of the identity.

In order to prove the last part of the theorem, we observe that the singular integral operators and their adjoints are defined in all spaces L^p, $1 < p < \infty$, and continuous in the corresponding topologies. Therefore an operator K in $\mathfrak{A}_p$ will map $L^p \cap L^q$ into itself, and since $L^p \cap L^q$ is dense in L^q, the restriction of K to $L^p \cap L^q$ will have a unique continuous extension to L^q, which we take as the definition of $\phi(K)$. Then one verifies that ϕ is the desired isomorphism between $\mathfrak{A}_p$ and $\mathfrak{A}_q$.

Theorem 6 is thus established.

THEOREM 7. *Let* $\alpha = (\alpha_1, \cdots, \alpha_k)$ *be a k-tuple of non-negative integers and write* $D_\alpha u = \partial^{\alpha_1+\cdots+\alpha_k} u/\partial x_1^{\alpha_1}\partial x_2^{\alpha_2}\cdots\partial x_k^{\alpha_k}$, $z^\alpha = z^{\alpha_1} z_2^{\alpha_2}\cdots z_n^{\alpha_n}$. *Let* $P(u) = \sum a_\alpha(x) D_\alpha u$ *be a linear partial differential operator of homogeneous order m with coefficients* $a_\alpha(x)$ *in* C_β, $\beta \geqq 0$. *Then if* $u \in L_m^p$, $P(u) = H\Lambda^m u$ *where* H *is a singular integral operator of type* C_β^∞ *and*

$$\sigma(H) = (-i)^m \sum_\alpha a_\alpha(x) z^\alpha |z|^{-m}, \text{ where } |z| = (z_1^2 + \cdots + z_k^2)^{\frac{1}{2}}.$$

According to (23), we have $\partial u/\partial x_n = -iR_n \Lambda u$ and therefore, since the R_n and Λ commute, it follows that

$$D_\alpha u = (-i)^m R_1^{\alpha_1} R_2^{\alpha_2} \cdots R_k^{\alpha_k} \Lambda^m u = (-i)^m R^\alpha \Lambda^m u$$

and

$$P(u) = \sum_\alpha a_\alpha(x) D_\alpha u = (-i)^m \sum a_\alpha(x) R^\alpha \Lambda^m u.$$

Now according to (14) and (37), $\sigma(R_n) = z_n |z|^{-1}$ and from this the desired expression for

$$\sigma(H) = \sigma[(-i)^m \sum_\alpha a_\alpha(x) R^\alpha]$$

follows. This proves the theorem.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY,
CORNELL UNIVERSITY,
UNIVERSITY OF CHICAGO.

REFERENCES.

[1] H. Bateman, *Higher transcendental functions*, vol. 2, N. Y., 1953.

[2] S. Bochner, "Theta relations with spherical harmonics," *Proceedings of the National Academy of Sciences*, vol. 37 (1951), pp. 804-808.

[3] A. P. Calderón and A. Zygmund, "On singular integrals," *American Journal of Mathematics*, vol. 78 (1956), pp. 289-309.

[4] E. Heine, *Handbuch der Kugelfunktionen*, vols. I and II, 2d. ed., Berlin, 1878-1888.

[5] G. N. Watson, *A treatise on the theory of Bessel functions*, Cambridge University Press, 1922.

ON SIMPLE GROUPS OF TYPE B_n.*

By JEAN DIEUDONNÉ.

1. C. Chevalley [1] has recently defined simple linear groups over an arbitrary field K, corresponding to the classes of simple Lie algebras over the complex field; and, with one exception, R. Ree [4] has identified the groups corresponding to the classes A_n, B_n, C_n, D_n and G_2 to well-known classical groups. The exception concerns the class B_n when $n \geqq 2$ and K is an imperfect field of characteristic 2; I will prove in this note, using Ree's other results and the general structure of orthogonal groups corresponding to defective quadratic forms [2, pp. 52-60], that in that exceptional case the Chevalley group is again isomorphic to *the commutator subgroup of the orthogonal group defined by the quadratic form* $Q(x) = \sum_{i=0}^{n} \xi_i \xi_{-i}$ (with respect to a suitable basis $(e_i)_{-n \leqq i \leqq n}$ of a $(2n+1)$-dimensional space E over K).

2. It is proved in [4, p. 398] that the Chevalley group of type B_n leaves invariant the $2n$-dimensional subspace E_1 of E generated by the e_i of index $\neq 0$, and is isomorphic to its restriction H to that subspace. Moreover, H is generated by the matrices

$$V_{i,t} = I + t^2 E_{-ii} \text{ and } W_{i,j,t} = I + t(E_{i,-j} - E_{j,-i}),$$

where $t \in K$, and i, j take the values $\pm 1, \pm 2, \cdots, \pm n$, the E_{ij} being as usual the matrices such that $E_{ij} \cdot e_j = e_i$, $E_{ij} \cdot e_k = 0$ for $k \neq j$. Now, in the case we are considering, the K^2-subspace $\mathfrak{M}$ of K from the general theory of defective forms [2, p. 52] is reduced to K^2; therefore, for fixed i, the $V_{i,t}$ constitute *all singular orthogonal transvections* [2, p. 55] corresponding to the vector e_{-i}. But, for fixed i, the $V_{i,t}$ and $V_{-i,t}$ obviously generate the unimodular group $SL_2(K^2)$ corresponding to the K^2-plane P_i generated by e_i and e_{-i}; there is therefore in that group a matrix U which transforms e_{-i} into a vector $a \in P_i$ such that $Q(a) \neq 0$; furthermore $Q(a) \in K^2$, hence the transformations $UV_{i,t}U^{-1}$ constitute *all semi-singular orthogonal transvections* [2, p. 54] corresponding to the vector a.

---

* Received May 21, 1957.

Next we remark that, as $n \geqq 2$, the subgroup generated by the matrices $W_{i,j,t}$ contains the commutator subgroup $\Omega_{2n}(K, Q_1)$, where Q_1 is the restriction to E_1 of the quadratic form Q [4, p. 397]. But from Witt's theorem it is easy to deduce that for any vector $b \in E_1$ such that $Q(b) \in K^2$ and $Q(b) \neq 0$, there is a transformation of $\Omega_{2n}(K, Q_1)$ transforming a into a scalar multiple of b, and that for any vector $c \in E_1$ such that $Q(c) = 0$, there is a transformation of $\Omega_{2n}(K, Q_1)$ sending e_{-i} into a scalar multiple of c [3, § 10, 7), p. 65]. It follows that the group H contains *all* semi-singular transvections, and therefore the commutator subgroup $\Omega_{2n+1}(K, Q)$ ([2], p. 59 and [3], § 11, p. 69); on the other hand, as $W_{i,j,t}$ belongs to the orthogonal group $O_{2n}(K, Q_1)$, and a fortiori to the orthogonal group $O_{2n+1}(K, Q)$, the group $\Omega_{2n+1}(K, Q)$ is a normal subgroup of H, and is not contained in the center of H; hence $H = \Omega_{2n+1}(K, Q)$.

It may be remarked that the theorem still holds when $n = 1$. Indeed, we have seen above that H is then the unimodular group $SL_2(K^2)$, hence H contains all semi-singular transvections corresponding to vectors $\xi_1 e_1 + \xi_{-1} e_{-1}$ such that $\xi_1 \xi_{-1} \in K^2$, and these are in fact all semi-singular transvections; the argument is then concluded as above.

NORTHWESTERN UNIVERSITY.

REFERENCES.

[1] C. Chevalley, "Sur certains groupes simples," *Tôhoku Math. J.*, (2), vol. 7 (1955), pp. 14-66.

[2] J. Dieudonné, "Sur les groupes classiques," *Actual. Scient. et Ind.*, no. 1040, Paris (Hermann), 1948.

[3] ———, *La géométrie des groupes classiques*, Erg. der Math., Neue Folge, Heft 5, Berlin (Springer), 1955.

[4] R. Ree, "On some simple groups defined by C. Chevalley," *Trans. Amer. Math. Soc.*, vol. 84 (1957), pp. 392-400.

EXTENSIONS OF REPRESENTATIONS OF LIE GROUPS AND LIE ALGEBRAS, I.*

By G. Hochschild ** and G. D. Mostow.†

1. Introduction.

Let K be a group, G a subgroup of K, ρ a representation of G, V the representation space of ρ. We shall say that a representation σ of K is an extension of the representation ρ of G if the representation space W of σ contains V as a G-stable subspace and σ coincides with ρ in V. If we insist on remaining within the category of *finite dimensional* representations, such an extension does not always exist. In the case where G is normal in K and there is a complementary subgroup H in K such that K is a semidirect product $H \cdot G$, the extension problem for finite dimensional representations can be analyzed in terms of representative functions. In fact, using the representative functions associated with the given representation ρ of V, we shall give a standard construction yielding a representation space W for K such that W contains V as a G-stable subspace, *and is finite dimensional whenever such a representation space exists at all.* If K is a connected Lie group, and for the category of finite dimensional continuous representations, this gives a complete solution of the extendibility problem (Theorem 3.1). Moreover, we give a construction that enables us to treat the more general case where $K = HG$, with $H \cap G$ compact (Theorem 3.2).

In Section 4, we shall show how some of the basic result on the existence of faithful representations for connected Lie groups can be proved comparatively simply by means of the extension theorem. In particular, the use of Ado's theorem on the existence of a faithful representation for a Lie algebra is completely eliminated.

On the other hand, the extension theorem for representations has an analogue for Lie algebras, which is due to Zassenhaus and was used by him in proving Ado's theorem. The technique of representative functions, here defined as functions on the universal enveloping algebra, gives a very simple

---

* Received May 15, 1957.

** John Simon Guggenheim Fellow.

† Supported in part by a research contract with the U. S. Airforce.

and natural proof of Zassenhaus's extension theorem, and thus of Ado's theorem. We shall give this proof in Section 5, which is quite independent of what precedes.

2. Notation and general facts. Let F be a field, and let V be a vector space of finite dimension d over F. A representation ρ of a group G in V, or with representation space V, is a homomorphism of G into the group of all linear automorphisms of V. If $x \in G$ and $v \in V$, we abbreviate $\rho(x)(v)$ by $x \cdot v$. Let $E(V)$ denote the algebra of all linear endomorphisms of V. If λ is any linear map of $E(V)$ into F, the composite function $\lambda \circ \rho$ from G to F is called a *representative function* on G associated with the representation ρ. These functions make up a finite dimensional vector space $R(\rho)$ over F. If f is any function on G, and $x \in G$, we define the left translate $x \cdot f$ as the function on G that is given by $(x \cdot f)(y) = f(yx)$, for all $y \in G$. Similarly, the right translate $f \cdot x$ is defined by $(f \cdot x)(y) = f(xy)$. In particular, if $f \in R(\rho)$, then $x \cdot f$ and $f \cdot x$ belong to $R(\rho)$, for every $x \in G$. Using only the left translations, we thus have a natural representation of G in $R(\rho)$.

Let μ be any linear map of V into F, and let $v \in V$. Then we define a function $\mu/v \in R(\rho)$ by setting $(\mu/v)(y) = \mu(y \cdot v)$. Observe that $x \cdot (\mu/v) = \mu/x \cdot v$. Now let $\mu_1, \cdots, \mu_d$ be a basis for the dual space $\mathrm{Hom}_F(V, F)$ of V. Let $d \cdot R(\rho)$ stand for the direct sum of d copies of $R(\rho)$, regarded as a representation space for G in the natural fashion. We define a map of V into $d \cdot R(\rho) : v \rightarrow (\mu_1/v, \cdots, \mu_d/v)$. It is immediately verified that this is a G-monomorphism.

Let $V = V_0 \supset \cdots \supset V_n = (0)$ be a composition series for the representation space V. Let V' be the direct sum of the factor representation spaces V_i/V_{i+1}, where i ranges from 0 to $n - 1$. Then V' is a semisimple representation space for G. Moreover, to within G-isomorphisms, V' is independent of the particular choice of the composition series. Hence the representation ρ' of G in V' is essentially determined by ρ; we shall call it the *semisimple representation associated with* ρ. Clearly, if ρ is a semisimple representation, ρ' may be identified with ρ.

We shall say that a representation ρ of G is *unipotent* if the representation space V has a descending series of G-stable subspaces such that the representation in each factor space of the series is trivial. It amounts to the same thing to say that ρ' is trivial. More precisely, let K be a subgroup of G. Then, if ρ' is trivial on K, it clearly follows that ρ is unipotent on K. Conversely, *if K is normal in G*, and if ρ is unipotent on K, then

ρ' is trivial on K, because every semisimple representation space for G is then semisimple as a representation space for K.

Let 1 stand for the identity transformation on V, and let K be an arbitrary subgroup of G. It is easily seen that the representation ρ of G is unipotent on K if and only if there is a positive integer n such that, for every n-tuple $x_1, \cdots, x_n$ of elements of K,

$$(1-\rho(x_1)) \cdots (1-\rho(x_n)) = 0.$$

It is clear from this that, if ρ is unipotent on K, so is the representation of K in $R(\rho)$, since $\Pi(1-x_i) \cdot (\mu/v) = \mu/(\Pi(1-\rho(x_i)))(v)$. It is equally evident that a subrepresentation or a factor representation of a unipotent representation is unipotent. Similarly, a sum of unipotent representations is unipotent. Finally, the tensor product of two unipotent representations ρ and σ is unipotent, as is seen from the relation

$$1 \otimes 1 - \rho(x) \otimes \sigma(x) = (1-\rho(x)) \otimes 1 + \rho(x) \otimes (1-\sigma(x)).$$

It has been shown by Kolchin that ρ is unipotent if, for every $x \in G$, the transformation $1-\rho(x)$ is nilpotent. We remark that this follows readily from Wedderburn's theorem on simple algebras. Observe first that we may asume without loss of generality that F is algebraically closed. Next, note that if we proceed by induction on the dimension of V we reduce the problem to the case where V is a simple representation space for G. Now let A be the algebra of linear endomorphisms of V that is generated by the endomorphisms $1-\rho(x)$, with $x \in G$. Clearly, an A-stable subspace of V is also G-stable, so that V is simple as an A-module. Hence, if $A \neq (0)$, it follows from Wedderburn's theorem that A is the algebra of all linear transformations of V. On the other hand, we see immediately that every element of A is actually a finite linear combination of elements $1-\rho(x)$, with $x \in G$. If every such element is nilpotent it follows that every element of A has trace 0. Hence A cannot contain every linear transformation of V, and therefore must be (0).

3. Extensions of representations. Let G be a Lie group. By a representation of G we shall mean a continuous representation by linear transformations of a finite dimensional vector space over the field of the real numbers. The radical of G is defined as the unique maximum solvable normal analytic subgroup of G. It is closed in G, and its Lie algebra is the radical (maximum solvable ideal) of the Lie algebra of G.

LEMMA 3.1. *Let G be a connected Lie group, R the radical of G, S a* *maximal semisimple analytic subgroup of* G. *Let* ρ *be a representation of* G, *and let* A *be a set of analytic automorphisms* a *of* G *such that* (1) : *for every* $x \in R$, $\rho'(a(x)x^{-1}) = 1$, *and* (2) : *for every* $x \in S$, $\rho(a(x)x^{-1}) = 1$. *Then, if* f *is any representative function associated with* ρ, *the space spanned by the functions* $f \circ a$, *with* $a \in A$, *is finite dimensional.*

Proof. First we show that we may assume G to be simply connected. Let G^+ be the simply connected covering group of G, and let $p\colon G^+ \to G$ be the covering epimorphism. Then $f \circ p$ is a representative function on G^+ that is associated with the representation $\rho \circ p$ of G^+. The map $f \to f \circ p$ is evidently a linear monomorphism of the space of functions on G into that of G^+. Hence it suffices to show that the space spanned by the functions $f \circ a \circ p$, with $a \in A$, is finite dimensional. Now, for every $a \in A$, there is one and only one analytic automorphism a^+ of G^+ such that $p \circ a^+ = a \circ p$. We have $f \circ a \circ p = f \circ p \circ a^+$. Clearly, $\rho' \circ p$ is the semisimple representation of G^+ that is associated with the representation $\rho \circ p$ of G^+. If R^+ is the radical of G^+, then $p(R^+) = R$. For $x \in R^+$, we have $(\rho' \circ p)(a^+(x)x^{-1}) = \rho'(a(p(x))p(x)^{-1}) = 1$. Similarly, there is a maximal semisimple analytic subgroup S^+ of G^+ such that $p(S^+) = S$, and if $x \in S^+$, we have $(\rho \circ p)(a^+(x)x^{-1}) = \rho(a(p(x))p(x)^{-1}) = 1$. Hence the automorphisms a^+ satisfy the conditions of our lemma for the representation $\rho \circ p$ of G^+. Hence it suffices to prove the lemma in the case where G is simply connected, which we shall now assume.

Then G is the semidirect product $S \cdot R$. Let $\mathfrak{R}$ be the Lie algebra of R, and let $\mathfrak{T}$ be the Lie algebra of the kernel of ρ' in R. Since R is normal in G, ρ' yields a semisimple representation of R, and its differential yields a semisimple representation of $\mathfrak{R}$. Hence we may apply Lie's theorem to conclude that $[\mathfrak{R}, \mathfrak{R}] \subset \mathfrak{T}$. Let $x_1, \cdots, x_n$ be representatives in $\mathfrak{R}$ for a basis of $\mathfrak{R}/\mathfrak{T}$. Then $\mathfrak{T} \subset (\mathfrak{T}, x_1) \subset \cdots \subset (\mathfrak{T}, x_1, \cdots, x_n) = \mathfrak{R}$ is a sequence of ideals of $\mathfrak{R}$. Since R is simply connected, the analytic subgroup T of R that corresponds to the ideal $\mathfrak{T}$ of $\mathfrak{R}$ is closed in R and simply connected.[1] Since $\mathfrak{T}$ is nilpotent, the exponential map is a homeomorphism of $\mathfrak{T}$ into T.[2] Moreover, R can be reached from T by successively constructing semidirect products according to our series of ideals from $\mathfrak{T}$ to $\mathfrak{R}$. Hence we have a homeomorphism ψ of $\mathfrak{N}$ onto R, where, for $u \in \mathfrak{T}$ and real numbers t_i, $\psi(u + \sum_{i=1}^{n} t_i x_i) = \exp(u)\exp(t_1 x_1) \cdots \exp(t_n x_n)$.

---

[1] According to a well known result due to Malcev, every normal analytic subgroup of a simply connected Lie group is closed and simply connected. The proof is obtained by reconstructing the group through a sequence of semidirect products, as is done below for R in order to define ψ.

[2] This well known result is proved by induction on the length of the ascending central series for $\mathfrak{T}$, using the result of footnote 1.

Every analytic automorphism $a \in A$ induces an automorphism $a\cdot$ of $\mathfrak{N}$. It follows from condition (1) that we have $a\cdot(\mathfrak{T}) \subset \mathfrak{T}$, and $a\cdot(x_i) = a_i + x_i$, with $a_i \in \mathfrak{T}$, for each i. If $z = u + \sum_{i=1}^{n} t_i x_i$, we have therefore

$$a(\psi(z)) = \exp(a\cdot(u))\exp(t_1(a_1 + x_1)) \cdots \exp(t_n(a_n + x_n)).$$

Now let $\rho\cdot$ stand for the representation of $\mathfrak{N}$ that is induved by ρ, and write $\alpha_i = \rho\cdot(a_i)$, $\zeta_i = \rho\cdot(x_i)$. Then we have

$$\rho(a(\psi(z))) = \exp(\rho a\cdot(u))\exp(t_1(\alpha_1 + \zeta_1)) \cdots \exp(t_n(\alpha_n + \zeta_n)).$$

Choose a basis $y_1, \cdots, y_q$ for $\mathfrak{T}$, and write $a\cdot(y_j) = \sum_{k=1}^{q} b_{jk} y_k$, and $a_i = \sum_{k=1}^{q} a_{ik} y_k$. Then $\alpha_i = \sum_{k=1}^{q} a_{ik}\eta_k$, where $\eta_k = \rho\cdot(y_k)$.

The representation $\rho\cdot$ is nilpotent on $\mathfrak{T}$, and $\rho\cdot(\mathfrak{T})$ is an ideal in $\rho\cdot(\mathfrak{N})$. It follows that, if d is the dimension of the representation space V of ρ, every monomial in elements of $\rho\cdot(\mathfrak{N})$ in which there occur more than $d - 1$ factors in $\rho\cdot(\mathfrak{T})$ is 0.

Writing out the exponential series in our expression for $\rho(a(\psi(z)))$, we obtain the absolutely convergent series

$$\sum (\rho a\cdot(u))^{e}(\alpha_1 + \zeta_1)^{e_1} \cdots (\alpha_n + \zeta_n)^{e_n} t_1^{e_1} \cdots t_n^{e_n}(e!e_1! \cdots e_n!)^{-1},$$

where the summation goes over all $(n+1)$-tuples $(e, e_1, \cdots, e_n)$ of non-negative integers, with $e < d$. Write $u = \sum_k c_k y_k$, so that $\rho a\cdot(u) = \sum_{j,k} b_{kj} c_k \eta_j$. Now substitute this for $\rho a\cdot(u)$, and $\sum_k a_{ik}\eta_k$ for α_i, in the above, and then multiply out each term of the series in full. Each term can be written in the form $p_1 q_1(e, e_1, \cdots, e_n) + \cdots + p_r q_r(e, e_1, \cdots, e_n)$, where the p_i are the various monomials of degree $\leqq e + e_1 + \cdots + e_n$ in the coefficients b_{kj} and a_{ik} of $a\cdot$, and the $q_i(e, e_1, \cdots, e_n)$ are certain homogeneous (non-commutative) polynomials in the η_j and ζ_i whose coefficients depend on the t_i and the c_k, i.e., on z, but not on the automorphism a. It is easily seen by the usual estimate of the size of the elements of a product of matrices that, for each i, the series $\sum_{(e, e_1, \cdots, e_n)} q_i(e, e_1, \cdots, e_n)$ is absolutely convergent. Moreover, it is clear from our remark above that $q_i(e, e_1, \cdots, e_n) = 0$ whenever p_i is of degree greater than $d - 1$. Hence we conclude that, if $p_1, \cdots, p_s$ are all the monomials of degree $< d$ in the coefficients of $a\cdot$, there are certain

S, this map must be constant, whence we conclude that yur commutes with every element of S.

We extend the left G-translations of functions on G to K-operations on these functions: let f be a function on G, h an element of H, x and y elements of G. Then the function $(hx)\cdot f$ on G is defined by setting

$$((hx)\cdot f)(y) = f(h^{-1}yhx).$$

Clearly, if f is continuous, so is $(hx)\cdot f$. Furthermore, it is easily verified that $u\cdot(v\cdot f) = (uv)\cdot f$, for all u and v in K.

By what we have shown above, given any element $h \in H$, we can find an element $z \in G$ such that hz commutes with every element of S. Let a be the automorphism $x \rightarrow (hz)^{-1}x(hz)$. Then we have $h\cdot f = (z^{-1}\cdot f\cdot z)\circ a$.

Now suppose that $f \in R(\rho)$. By the assumption of our theorem, the automorphism a satisfies the conditions of Lemma 3.1. Since the functions $z^{-1}\cdot f\cdot z$ lie in the finite dimensional space $R(\rho)$, it follows therefore from Lemma 3.1 that the space spanned by the functions $h\cdot f$, as h ranges over H and f ranges over $R(\rho)$, is finite dimensional. Hence the K-transforms of the elements of $R(\rho)$ make up a finite dimensional space U of functions on G, and U is a representation space for K containing $R(\rho)$ as a G-stable subspace. We have seen in Section 2 that there is a G-monomorphism of V into $d\cdot R(\rho)$. Composing this with the injection $R(\rho)\rightarrow U$, we obtain a G-monomorphism of V into the representation space $d\cdot U$ for K. Let σ denote the representation of K in $d\cdot U$. There remains only to show that the kernel of σ' contains the kernel of ρ'.

It follows from the condition of our theorem that the kernel of ρ' is normal in K, not only in G. Indeed, let z be an element of the kernel of ρ', and let $y \in K$. We can write $z = sr$, with $s \in S$ and $r \in R$. As we have seen above, there is an element $u \in G$ such that uy commutes with every element of S. We have

$$yzy^{-1} = (ysy^{-1})(yry^{-1}) = (u^{-1}su)(yry^{-1}) = (u^{-1}zu)(u^{-1}r^{-1}u)(yry^{-1}).$$

Since the kernel of ρ' is normal in G, we have $\rho'(u^{-1}zu) = 1$. Applying ρ' to the last expression for yzy^{-1}, and using the condition of our theorem, we find therefore $\rho'(yzy^{-1}) = 1$, and we have shown that the kernel of ρ' is normal in K.

Hence it suffices to show that the representation of the kernel of ρ' in U is unipotent. The elements of U are linear combinations of function $y\cdot f$, with $y \in K$ and $f \in R(\rho)$. If z lies in the kernel of ρ', so does each conjugate $y^{-1}zy$, and we have $z\cdot(y\cdot f) = y\cdot(y^{-1}zy\cdot f)$. Since, as we have seen in Section 2, the representation of the kernel of ρ' in $R(\rho)$ is unipotent, this shows that the representation of the kernel of ρ' in U is unipotent. This completes the proof of Theorem 3.1.

Although we shall need Theorem 3.1 only in the form stated above, we point out the following generalization.

THEOREM 3.2. *Let K be a connected Lie group, G a closed connected normal subgroup of K, ρ a representation of G satisfying the condition of Theorem* 3.1. *Suppose that H is an analytic subgroup of K such that $K=HG$ and $H\cap G$ is a compact subgroup of the analytic group H. Assume that there is a representation of H that is faithful on $H\cap G$. Then ρ can be extended to a representation τ of K such that the kernel of τ' contains the kernel of ρ'.*

Proof. We construct the appropriate semidirect product $H\cdot G$, so that we have the natural epimorphism $H\cdot G\rightarrow HG=K$, whose kernel consists of the elements $x\cdot x^{-1}$, with $x\in H\cap G$. Let W be the representation space for the semidirect product $H\cdot G$, as defined in the proof of Theorem 3.1. The right translations of representative functions give us the structure of a right G-module on W, because W is a direct sum of copies of a space of representative functions on G that is stable under the right translations.

Now let A denote the group algebra, over the real number field, of the group $H\cap G$. The right G-module structure of W allows us to regard W as a right A-module. Let U be a representative space for H. Then we may also regard U as a left A-module, and we can form the tensor product $W\otimes_A U$. This is the canonical homomorphic image of the tensor product $W\otimes U$ over the real number field, the kernel consisting of all finite sums of elements of the form $w\cdot x\otimes u-w\otimes x\cdot u$, where $w\in W$, $u\in U$, and $x\in H\cap G$. Clearly, $W\otimes U$ is a representation space for $H\cdot G$ such that, with $h\in H$ and $g\in G$,

$$(h\cdot g)\cdot(w\otimes u)=((h\cdot g)\cdot w)\otimes(h\cdot u),$$

where $h\cdot g$ stands for the product of h and g in the semidirect product $H\cdot G$, not in K. It is easily verified that $(h\cdot g)\cdot(w\cdot x)=((h\cdot g)\cdot w)\cdot hxh^{-1}$, while $h\cdot(x\cdot u)=(hxh^{-1})\cdot(h\cdot u)$. Hence we see that the kernel of the canonical epimorphism $W\otimes U\rightarrow W\otimes_A U$ is stable under the operations with the elements of $H\cdot G$, so that we obtain the structure of a representation space for $H\cdot G$ on $W\otimes_A U$. Moreover, if $x\in H\cap G$, we have $(x\cdot x^{-1}\cdot w=w\cdot x^{-1}$, whence we see that the representation of $H\cdot G$ in $W\otimes_A U$ is trivial on the kernel of the epimorphism $H\cdot G\rightarrow K$. Thus we obtain a representation of K in $W\otimes_A U$.

Let η be a representation of H by *complex* linear automorphisms that is faithful on $H \cap G$. Since $H \cap G$ is compact, the restriction of η to $H \cap G$ and the dual representation of $H \cap G$ generate *all* representations of $H \cap G$, by the processes of forming direct sums, tensor products, and subrepresentations. This well known fact is the content of Prop. 3, p. 190, in [0]. It follows that every representation space for $H \cap G$ is an $H \cap G$—subspace of some representation space for H.

Now let J denote the set of all elements $a \in A$ such that $w \cdot a = 0$, for every $w \in W$. Then J is a two-sided ideal of A, and A/J is finite dimensional. Regard A/J as a representation space for $H \cap G$. The natural anti-monomorphism of A/J into $E(W)$ shows that the representation of $H \cap G$ in A/J is continuous. By what we have seen above, there is a representation space U for H that contains A/J as an $H \cap G$—stable subspace. As a representation space for $H \cap G$, U is semisimple, so that U is the direct sum of A/J and another $H \cap G$-stable subspace P. Thus we have the direct decomposition

$$W \otimes_A U = W \otimes_A (A/J) + W \otimes_A P,$$

and each of the two direct summands on the right is clearly a G-stable subspace of $W \otimes_A U$. Moreover, since J annihilates W from the right, the first summand is canonically isomorphic with W, as a representation space for G.

Thus, if τ is the representation of K in $W \otimes_A U$, then τ is an extension of the given representation ρ of G, via the representation of G in $W = W \otimes_A (A/J) \subset W \otimes_A U$. Furthermore, since the kernel of σ' (where σ is the representation of $H \cdot G$ in W) contains the kernel of ρ', and since, for $x \in G$, $x \cdot (w \otimes u) = (x \cdot w) \otimes u$, it follows that the kernel of τ' contains the kernel of ρ'. This completes the proof of Theorem 3.2.

Observe that *the condition imposed on ρ in the statement of Theorem 3.1 is necessary for ρ to be extendible to a representation of K.* Indeed, the commutators $yxy^{-1}x^{-1}$, where $y \in K$ and $x \in R$, belong to the connected component of the identity in the intersection of the commutator subgroup of G with R, on which every representation of K must be unipotent, by Lie's theorem.

Let K be a group, G a normal subgroup of K, H a subgroup of K such that $K = HG$ (not necessarily semidirect). We remark that if a representation ρ of K is unipotent on G and on H then ρ is unipotent. In showing this, let us operate with the group algebra of K. Let $h \in H$, $x \in G$. We have

$$(1-hx)=h(1-x)+(1-h), \text{ and } (1-x)h=h(1-h^{-1}xh).$$

Hence a product of such elements, $(1-h_1x_1)\cdots(1-h_qx_q)$, can be written as a sum of products of the form hu, where $h\in H$ and u is a product whose factors are either of the form $1-x$, with $x\in G$, or of the form $1-h$, with $h\in H$, the total number of factors being q. We have

$$(1-x)(1-h)=(1-x)-h(1-h^{-1}xh).$$

Hence each u can be rewritten as an integral linear combination of products of the form $h(1-h_1)\cdots(1-h_s)(1-x_1)\cdots(1-x_t)$, where h and the h_i are in H, the x_i are in G, and t is the number of factors of the form $1-x$, with $x\in G$, that occurred in the original form of u. Hence the endomorphism that corresponds to u in our representation ρ is 0 whenever t exceeds $d-1$, where d is the dimension of the representation space of ρ. On the other hand, if $t<d$ and $q\geqq d^2$, u must contain at least d *successive* factors of the form $1-h$, so that the corresponding endomorphism must again be 0. Thus the endomorphism corresponding to $(1-h_1x_1)\cdots(1-h_qx_q)$ is 0 whenever $q\geqq d^2$, which means that ρ is unipotent.

LEMMA 3.2. *In the situation of Theorem* 3.1, *suppose that G is simply connected and nilpotent, and that ρ is a unipotent representation of G. Assume also that the representation of H in the Lie algebra $\mathfrak{G}$ of G that is obtained from the adjoint representation of K is unipotent. Then the representation σ of K that is constructed in the proof of Theorem* 3.1 *is unipotent.*

Proof. The exponential map is a homeomorphism of $\mathfrak{G}$ onto G. Furthermore, if f is any element of the representation space U for K that we have constructed in the proof of Theorem 3.1, the composite map $f\circ\exp$ is a polynomial function on $\mathfrak{G}$ of degree $<d$, where d is the dimension of the representation space V of ρ; since $f\circ\exp=\lambda\circ\rho\circ\exp=\lambda\circ\exp\circ\rho^{\cdot}$, where λ is a linear function on $E(V)$. For every $h\in H$, we have

$$(h\cdot f)\circ\exp=f\circ\exp\circ(h^{-1})^{\cdot}.$$

Since the representation of H in $\mathfrak{G}$ is unipotent, so is the dual representation with operations $\mu\to\mu\circ(h^{-1})^{\cdot}$ in the space of the linear functions on $\mathfrak{G}$. The space of the polynomial functions of degree $<d$ on $\mathfrak{G}$ is a homomorphic image of a direct sum of tensor powers of the space of the linear functions on $\mathfrak{G}$, whence we see that the representation of H in this space of polynomial functions is unipotent. The map $f\to f\circ\exp$ is an H-monomorphism of U into the space of these polynomial functions, so that we may conclude that

the representation of H in U is unipotent. Hence the representation σ of K in $d \cdot U$ is unipotent on H. We know from Theorem 3.1 that σ is unipotent on G. By what we have seen above, this implies that σ is unipotent.

4. Existence of faithful representations. The results of the preceding Section greatly facilitate the proofs for the known basic results on the existence of faithful representations of connected Lie groups. We shall sketch these proofs.

THEOREM 4.1. (E. Cartan). *Let G be a simply connected solvable Lie group, and let N be the maximum nilpotent normal analytic subgroup of G. Then there exists a faithful representation of G that is unipotent on N.*

Proof. Let Z be the connected component of the identity in the center of N (actually, it is known that the center of N is connected). Then Z is closed and normal in G, and Z is simply connected. Furthermore, Z is non-trivial (unless G is trivial) so that, making an induction on the dimension of G, we may assume that there is a faithful representation of G/Z that is unipotent on N/Z. This may be regarded as a representation ρ of G that is unipotent on N and whose kernel is precisely Z. On the other hand, Z is a vector group, and we can clearly find a faithful unipotent representation of Z. We can reach N from Z by making a sequence of constructions of semidirect products each of which statisfies the requirement of Lemma 3.2. Hence, by applying Lemma 3.2 at each level, we can extend our representation of Z to a unipotent representation of N. Now we can reach G from N by making a sequence of constructions of semidirect products. Since the commutator subgroup of G lies in N, we can apply Theorem 3.1 at each level to extend our representation of N to a representation σ of G that is unipotent on N and faithful on Z. The direct sum of ρ and σ satisfies the requirements of Theorem 4.1.

For the next proofs, we need the following two facts:

1. *If a semisimple connected Lie group has a faithful representation then its center is finite.*

2. *Let G be a Lie group, and let P be a finite normal subgroup of G. Then, if G has a faithful representation, so has G/P.*

1. is well known and easy to prove.[4] As to 2., note that if G is connected, then a finite normal subgroup is necessarily in the center of G. This is the only case we need, and it is covered by a result of Goto.[5] However, it seems

---

[4] Lemma 5, in [2].

[5] Lemma 8, in [3].

worth while pointing out the following proof, which establishes a result that is more general than either 2. or the result of Goto.

Let ρ be the given faithful representation of G, V the representation space of ρ, L the group of all linear automorphisms of V. Let N be the normalizer of $\rho(P)$ in L. Then N is an algebraic linear group, and $\rho(P)$ is a normal subgroup of N. Moreover, since $\rho(P)$ is finite, it is an algebraic subgroup of N. By a theorem of Chevalley,[6] there is a rational representation τ of N whose kernel is exactly $\rho(P)$. The representation $\tau \circ \rho$ of G has exactly P for its kernel, and thus yields a faithful representation of G/P.

THEOREM 4.2 (Goto).[7] *Let G be a connected Lie group, and let S be a maximal semisimple analytic subgroup of G. Suppose that S has a faithful representation, and that the radical T of the commutator subgroup G' of G is closed in G, and simply connected. Then G has a faithful representation.*

Proof. Let R be the radical of G. Then R/T is a connected abelian Lie group, whence $R/T = A \times V$, the direct product of a toroidal group A and a vector group V. Let M denote the full preimage of V in R. Since T and M/T are simply connected, M is simply connected. Now $R/M = A$, and, since A is compact and M is simply connected and solvable, it follows that R is a semidirect product $B \cdot M$.[8] By Theorem 4.1, there exists a faithful representation of M that is unipotent on the maximum nilpotent normal analytic subgroup of M. Since T is contained in this maximum nilpotent normal analytic subgroup, our representation is unipotent on T. Hence we can apply Theorem 3.1 to extend our representation of M to a representation of R that is faithful on M and unipotent on T. On the other hand, since B is compact, there is a representation of R whose kernel is precisely M. Taking the direct sum of these two representations of R, we obtain a faithful representation of R that is unipotent on T.

Now let $S \cdot R$ be the semidirect product in which the multiplication is given by $(s_1, r_1)(s_2, r_2) = (s_1 s_2, s_2^{-1} r_1 s_2 r_2)$. By Theorem 3.1, our faithful representation of R can be extended to a representation of $S \cdot R$.

Now observe that the kernel of the natural epimorphism of $S \cdot R$ onto G is contained in $(S \cap R) \cdot (S \cap R)$. Since $S \cap R$ is a discrete subgroup of the analytic group S, it is contained in the center of S. Since S has a faithful representation, the center of S is finite. Hence the kernel of the epimorphism $S \cdot R \rightarrow G$ is finite. By what we have said before stating Theorem 4.2, it suffices therefore to show that the semidirect product $S \cdot R$ has a faithful representation. We have already obtained a representation of $S \cdot R$ that is faithful on R. Using a faithful representation of S in addition, we obtain a faithful representation of $S \cdot R$. This completes the proof.

---

[6] Prop. 11, p. 119, in [1].

[7] Essentially, Th. 10, in [3].

[8] This result is easily proved by induction from the special case where M is a vector group, which is due to Iwasawa; the generalization is given as Lemma 8.1, in [5].

We remark that *the conditions of Theorem* 4.2 *are necessary for the existence of a faithful representation.*[9]

THEOREM 4.3 (Malcev).[10] *Let G be a connected Lie group, R the radical of G. Suppose that R has a faithful representation, and that one (and hence every) maximal semisimple analytic subgroup of G has a faithful representation. Then G has a faithful representation.*

Proof. By Lie's theorem, every representation of R is unipotent on the commutator subgroup R' of R. It follows that the image of R' under the representation is closed in the full linear group, and simply connected. Since R has a faithful representation, it follows that R' is closed in R, and simply connected. Hence we can proceed exactly as in the beginning of our proof of Theorem 4.2, using R' in the place of T, to show that R is a semidirect product $A \cdot M$, where A is a toroidal group and M is a simply connected normal closed subgroup of R that contains R'.

Let $\mathfrak{G}$, $\mathfrak{R}$, $\mathfrak{A}$ denote the Lie algebras of G, R, A, respectively. Since A is compact, the representation of A in $\mathfrak{G}$ that is obtained from the adjoint representation of G is semisimple. Hence $\mathfrak{G}$ is semisimple as an $\mathfrak{A}$-module, whence $\mathfrak{G}$ is the direct sum of the submodule $[\mathfrak{A}, \mathfrak{G}]$ and the centralizer $\mathfrak{P}$ of $\mathfrak{A}$ in $\mathfrak{G}$. Since $[\mathfrak{A}, \mathfrak{G}] \subset \mathfrak{R}$, we have therefore $\mathfrak{G} = \mathfrak{P} + \mathfrak{R}$. Now let $\mathfrak{S}$ be a maximal semisimple subalgebra of $\mathfrak{P}$. Clearly, $\mathfrak{S}$ is then also a maximal semisimple subalgebra of $\mathfrak{G}$. Now $\mathfrak{A} + [\mathfrak{R}, \mathfrak{R}]$ is an $\mathfrak{S}$-submodule of $\mathfrak{R}$, and $\mathfrak{A} \cap [\mathfrak{R}, \mathfrak{R}] = (0)$. Hence we can write the $\mathfrak{S}$-module $\mathfrak{R}$ as a direct sum $\mathfrak{A} + \mathfrak{B}$, where $\mathfrak{B}$ is an $\mathfrak{S}$-submodule containing $[\mathfrak{R}, \mathfrak{R}]$. Hence $\mathfrak{B}$ is an ideal of $\mathfrak{G}$, the corresponding analytic subgroup B of R is normal in G, and $R = AB$. Furthermore, our Lie algebra decomposition shows that the radical T of G' is contained in B, because the Lie algebra of T is $[\mathfrak{G}, \mathfrak{R}] = [\mathfrak{S}, \mathfrak{R}] + [\mathfrak{R}, \mathfrak{R}] = [\mathfrak{S}, \mathfrak{B}] + [\mathfrak{R}, \mathfrak{R}] \subset \mathfrak{B}$.

Now consider the natural epimorphism $B/R' \rightarrow R/(AR')$. The kernel of this epimorphism is the discrete subgroup $B/R' \cap (AR')/R'$ of the analytic group B/R'. On the other hand, the image $R/(AR')$ is isomorphic with M/R', which is a vector group. Hence $R/(AR')$ has no non-trivial covering, whence our epimorphism must be an isomorphism. Thus we have $B/R' \cap (AR')/R' = (1)$, and B/R' is simply connected. It is clear from the former that the natural epimorphism $(AR')/R' \times B/R' \rightarrow R/R'$ is an isomorphism. Consequently, B/R' is closed in R/R'. Hence B is closed in R, and therefore in G. In addition, B is simply connected, because both R' and B/R' are simply connected.

---

[9] See [3]; or Th. 7.3, in [5].

[10] [6]; or Th. 7, in [3].

As a normal analytic subgroup of the simply connected group B, the radical T of G' is closed in B, and simply connected. Hence it is clear that the assumptions of Theorem 4.2 are satisfied. We conclude from Theorem 4.2 that G has a faithful representation, and our proof is complete.

It is evident that the conditions of Theorem 4.3 are necessary for the existence of a faithful representation of G.

5. Faithful representations of Lie algebras.

Let L be a finite dimensional Lie algebra over a field F of characteristic 0, and let K be an ideal of L. We assume that there is a subalgebra H of L such that L is the semidirect sum $H+K$. Let $U(L)$, $U(K)$ denote the universal enveloping algebras of L, K, respectively. We define right L-operations on $U(K)$ as follows: let $u \in U(K)$, $h \in H$, $k \in K$. We define $u \cdot (h+k) = uh - hu + uk$, observing that, since K is an ideal of L, $uh - hu$ lies in $U(K)$, where we regard $U(K)$ as a subalgebra of $U(L)$ in the natural fashion. It can be verified immediately that, for arbitrary elements x and y of L, we have

$$(u \cdot x) \cdot y - (u \cdot y) \cdot x = u \cdot [x, y].$$

It follows that these right L-operators on $U(K)$ define the structure of a right $U(L)$-module on $U(K)$. We make the dual space $\mathrm{Hom}_F(U(K), F)$ into a left $U(L)$-module accordingly: $(x \cdot f)(u) = f(u \cdot x)$.

A representation ρ of K gives rise in the canonical fashion to a representation, which we still denote by ρ, of the associative algebra $U(K)$. If V is the representation space of ρ, and λ is any linear map of $E(V)$ into F, then the composite function $\lambda \circ \rho$ on $U(K)$ is called a *representative function* associated with ρ. As before, we shall always assume that V is finite dimensional.

The kernel of ρ in $U(K)$ is a two sided ideal I of $U(K)$. Since V is finite dimensional, $U(K)/I$ is finite dimensional, i.e., I is of finite codimension in $U(K)$. The representative functions associated with ρ vanish on I, and constitute a finite dimensional space $R(\rho)$ over F. Clearly, $R(\rho)$ is a $U(K)$-submodule (though not always a $U(L)$-submodule) of $\mathrm{Hom}_F(U(K), F)$.

$U(K)$ has a natural increasing filtration by the subspaces $U(K)_m$ $(m = 0, 1, \cdots)$ consisting of the elements that can be written as (noncommutative) polynomials of degree $\leqq m$ in the elements of $K(U(K)_0 = F)$. The associated graded algebra $\sum_m U(K)_m/U(K)_{m-1}$ is isomorphic with the symmetric algebra built over K, i. e., with a polynomial algebra in n variables, where n is the dimension of K. One verifies easily from this that $U(K)$ satisfies the maximal condition for ideals. On the other hand, one shows easily that, if A is any algebra, and I and J are ideals of finite codimension in A one of which is finitely generated as an A-module, then the product ideal IJ is of finite codimension in $U(K)$. Hence the important fact (first proved and utilized by Zassenhaus) that *the product of ideals of finite codimension in $U(K)$ is of finite codimension.*

In these terms, we can give a simple proof for the following extension theorem.

THEOREM 5.1 (Zassenhaus).[11] *Let L be a finite dimensional Lie algebra over a field F of characteristic* 0, *let K be an ideal of L, and suppose that L is a semidirect sum $H + K$, where H is a subalgebra. Let ρ be a finite dimensional representation of K, and suppose that $\rho'([H, K]) = (0)$, where ρ' is the semisimple representation associated with ρ. Then the representation space V of ρ can be K-monomorphically imbedded in a finite dimensional representation space W for L. If σ is the representation of L in W the kernel of σ' contains the kernel of ρ'. Furthermore, if H is nilpotent on K, under the adjoint representation, then $\sigma'(H) = (0)$.*

Proof. Let I, I' be the kernels of ρ, ρ', respectively, in $U(K)$. Then it is clear that $(I')^d \subset I$, where d is the dimension of V. Since $[H, K] \subset I'$, it follows that $uh - hu \in I'$, for every $u \in U(K)$ and every $h \in H$. Hence $(I')^d$ is a $U(L)$-submodule of $U(K)$. Hence, for every $f \in R(\rho)$ and every $x \in U(L)$, the function $x \cdot f$ vanishes on $(I')^{\alpha}$. Since, by what we have said above, $(I')^d$ is of finite codimension in $U(K)$, it follows that the $U(L)$-submodule S of $\mathrm{Hom}_F(U(K), F)$ that is generated by $R(\rho)$ is finite dimensional and is annihiliated by $(I')^d$.

Now (cf. § 2) we have a $U(K)$-monomorphism $V \to d \cdot R(\rho)$. Composing this with the injection $R(\rho) \to S$, we obtain a $U(K)$-monomorphism $V \to d \cdot S = W$. Since $(I')^d$ annihilates S, our representation σ of L in W is nilpotent on the ideal $I' \cap K$ of L. Hence, using that, for any ideal P of L, and any L-module M, $P \cdot M$ is an L-submodule of M, we conclude that the associated semisimple representation σ' annihilates $I' \cap K$, i.e., the kernel of σ' contains the kernel of ρ'.

---

[11] See [7], which also establishes the required facts concerning the universal enveloping algebra.

Now suppose that H is nilpotent on K. Then, for every $u \in U(K)$, there is an integer n such that $u \cdot (h_1 \cdots h_n) = 0$, for all $h_i \in H$. Since $U(K)/(I')^d$ is finite dimensional, this shows that the (anti-)representation of H in $U(K)/(I)^d$ is nilpotent, whence the representation of H in S is nilpotent. Thus our representation σ is nilpotent on the ideal $I' \cap K$ and on the subalgebra H. By an elementary combinatorial argument (easier than the group analogue of § 3), it follows that σ is nilpotent on $H + I' \cap K$. Since this is an ideal of L, it must therefore be contained in the kernel of σ'. This completes the proof of Theorem 5.1.

The existence of a faithful representation for a finite dimensional Lie algebra L over a field F of characteristic 0 is easily deduced from Theorem 5.1. Let N be the maximum nilpotent ideal of L, R the radical of L, S a maximal semisimple subalgebra of L. We shall prove that *there is a faithful representation of L that is nilpotent on N.*

Let Z be the center of L. The adjoint representation of L is nilpotent on N and has kernel Z. There is a chain $N = N_0 \supset \cdots \supset N_r = Z$ of ideals of N such that each N_i/N_{i+1} is 1-dimensional, so that N_i is a semidirect sum of N_{i+1} and the 1-dimensional Lie algebra. Starting with a faithful nilpotent representation of Z, we apply Theorem 5.1 repeatedly to construct a nilpotent representation of N that is faithful on Z.

Now there is a chain $R = R_0 \supset \cdots \supset R_q = N$ of ideals of R such that each R_j/R_{j+1} is 1-dimensional. Using only the first part of Theorem 5.1, noting that $[R, R] \subset N$, we extend our representation of N to a representation of R that is still nilpotent on N and faithful on Z.

Finally, since L is the semidirect sum $S + R$ and $[S, R] \subset N$, we can extend our representation of R to a representation of L that is nilpotent on N and faithful on Z. The direct sum of this representation and the adjoint representation satisfies our requirements.

6. Correspondence between representative functions.

Let G be a connected Lie group, let $\mathfrak{G}$ be the Lie algebra of G, and let $U(\mathfrak{G})$ be the universal enveloping algebra of $\mathfrak{G}$. Let A be the algebra of all real analytic functions on G. The elements of $\mathfrak{G}$ are left invariant infinitesimal transformations on G, in the sense of § II, Ch. IV of [0]. Hence A has the structure of a $\mathfrak{G}$-module, the elements of $\mathfrak{G}$ acting as derivations on A that commute with the right translations. Accordingly, we may regard A as a left $U(\mathfrak{G})$-module.

For an element u of $\mathfrak{G}$, we denote by e_u the corresponding homomorphism of the additive group R of the real line into G, i.e., $e_u(r) = \exp(ru)$, for every real number r. Let $f \in A$, $x \in G$, and put $g(r) = (x \exp(ru))$. Then g is a real analytic function on R, and it follows from the definition of the exponential map exp that the n-th derivative $g^{(n)}$ of g is equal to $(u^n \cdot (f \cdot x)) \circ e_u$ where u^n is the n-th power of u in $U(\mathfrak{G})$. Since the $U(\mathfrak{G})$-operations on A commute with the right translations, we have $g^{(n)} = ((u^n \cdot f) \cdot x) \circ e_u$. Hence, for all r in a sufficiently small neighborhood of 0 in R,

$$f(x \exp(ru)) = \sum_{n=0}^{\infty} (u^n \cdot f)(x) \cdot r^n/n!$$

Now, for every $f \in A$, let us define the function $f^{\cdot}$ on $U(\mathfrak{G})$ by setting $f^{\cdot}(u) = (u \cdot f)(1)$, for every $u \in U(\mathfrak{G})$, where 1 denotes the identity element of G. Clearly, the map $f \rightarrow f^{\cdot}$ is a linear map of A into the dual space $\mathrm{Hom}_R(U(\mathfrak{G}), R)$ of $U(\mathfrak{G})$. Moreover, if $f^{\cdot} = 0$, we conclude from the above that, for every $u \in \mathfrak{G}$, $f \circ e_u$ vanishes on some neighborhood of 0 in R, whence we conclude that f vanishes on some neighborhood of 1 in G. Since f is analytic everywhere on G, and since G is connected, this implies that $f = 0$. Thus our map $f \rightarrow f^{\cdot}$ is a linear monomorphism.

Now let ρ be a representation of G, and let V be the representation space of ρ. Let $f = \lambda \circ \rho$ be a representative function on G that is associated with ρ, i.e., λ is a linear function on $E(V)$. Let $\rho^{\cdot}$ be the representation of $U(\mathfrak{G})$ in V that is induced by ρ. We claim that $(\lambda \circ \rho)^{\cdot} = \lambda \circ \rho^{\cdot}$. The proof is as follows.

Let $x \in G$, $u \in \mathfrak{G}$. We have

$$(u \cdot (\lambda \circ \rho))(x) = ((u \cdot (\lambda \circ \rho)) \cdot x)(1) = (u \cdot ((\lambda \circ \rho) \cdot x))(1) = (u \cdot ((\lambda \cdot \rho(x)) \circ \rho))(1),$$

where $\lambda \cdot \rho(x)$ is the linear function on $E(V)$ that is defined by $(\lambda \cdot \rho(x))(e) = \lambda(\rho(x)e)$. By the above, with r in a neighborhood of 0 in R,

$$((\lambda \cdot \rho(x)) \circ \rho)(\exp(ru)) = \sum_{n=0}^{\infty} (u^n \cdot ((\lambda \cdot \rho(x)) \circ \rho))(1) \cdot r^n/n!.$$

The expression on the left can be written $\lambda(\rho(x) \exp(r\rho^{\cdot}(u)))$. If we expand this in a power series in r, and then compare the coefficients of r on the two sides above, we find that

$$\lambda(\rho(x)\rho^{\cdot}(u)) = (u \cdot (\lambda \cdot \rho(x)) \circ \rho))(1).$$

Hence we see from the first result of this proof that $u \cdot (\lambda \circ \rho) = (\rho^{\cdot}(u) \cdot \lambda) \circ \rho$, where $(\rho^{\cdot}(u) \cdot \lambda)(e) = \lambda(e\rho^{\cdot}(u))$. Clearly, this last result generalizes immediately to arbitrary elements u of $U(\mathfrak{G})$. Evaluating these functions at 1, we obtain $(\lambda \circ \rho)^{\cdot}(u) = \lambda(\rho^{\cdot}(u))$, which is the result to be proved.

Let W be a finite dimensional space consisting of representative functions on G, and suppose that W is stable under the left translations, so that W is a representation space for G. Let τ denote the representation of G in W, and let $\tau^{\cdot}$ be the induced representation of $U(\mathfrak{G})$ in W. If $u \in \mathfrak{G}$, and r is any real number, the left translation on W that is effected by the element $\exp(ru)$ of G is then given by $\exp(r\tau^{\cdot}(u))$. Thus we have, for every $x \in G$ and every $f \in W$,

$$f(x \exp(ru)) = \sum_{n=0}^{\infty} (\tau^{\cdot}(u))^n (f)(x) \cdot r^n/n!.$$

Comparing this with our general result (for r in some neighborhood of 0 in R) we find that $\tau^{\cdot}(u)(f) = u \cdot f$, for every $f \in W$ and every $u \in \mathfrak{G}$. This generalizes immediately to arbitrary elements $u \in U(\mathfrak{G})$. Thus W is a $U(\mathfrak{G})$-stable subspace of A, and the $U(\mathfrak{G})$-module structure of W that is induced by that of A coincides with the $U(\mathfrak{G})$-module structure given by $\tau^{\cdot}$. In particular, it follows immediately from this that the image $W^{\cdot}$ of W under the map $f \rightarrow f^{\cdot}$ is a $U(\mathfrak{G})$-submodule of $\mathrm{Hom}_R(U(\mathfrak{G}), R)$, for the module structure we have defined at the beginning of Section 5, and that this $U(\mathfrak{G})$-module structure of $W^{\cdot}$ coincides with the structure that is obtained by transporting $\tau^{\cdot}$ to $W^{\cdot}$ through the isomorphism $f \rightarrow f^{\cdot}$.

Now let us consider a semidirect product $H \cdot G$ and a representation ρ of G, as in Theorem 3.1. We have $R(\rho)^{\cdot} = R(\rho^{\cdot})$, by the above. In the proof of Theorem 3.1 we have obtained a representation space U for $H \cdot G$. U is the space of representative functions on G that is spanned by the transforms $h(f)$, with $h \in H$ and $f \in R(\rho)$, where $h(f)(x) = f(h^{-1}xh)$. Let a_h denote the conjugation with h in G, i.e., $a_h(x) = hxh^{-1}$. Then $h(f) = f \circ (a_h)^{-1}$. Let $h^{\cdot}$ denote the automorphism of $\mathfrak{G}$ that is induced by a_h. Then we have, with $u \in \mathfrak{G}$,

$$u \cdot (h(f)) = u \cdot (f \circ (a_h)^{-1}) = ((h^{-1})^{\cdot}(u) \cdot f) \circ (a_h)^{-1} = h((h^{-1})^{\cdot}(u) \cdot f).$$

Passing to the induced Lie algebra representation of the Lie algebra $\mathfrak{H}$ of H, we deduce that, with $v \in \mathfrak{H}$,

$$u \cdot (v(f)) = v(u \cdot f) + [u, v] \cdot f.$$

This generalizes immediately to arbitrary elements $u \in U(\mathfrak{G})$, where $[u, v] = uv - vu$. Since, for every $f \in U$, $h(f)(1) = f(1)$, for every $h \in H$, we have $v(f)(1) = 0$, for every $v \in \mathfrak{H}$. Hence, evaluating the above at 1, we find that $(v(f))^{\cdot}(u) = f^{\cdot}([u, v])$.

Thus our isomorphism $f \rightarrow f^{\cdot}$ transports the $\mathfrak{H}$-operations on U to the $\mathfrak{H}$-operations we have defined at the beginning of Section 5. Since U is the $\mathfrak{H}$-module generated by $R(\rho)$, it follows that $U^{\cdot}$ is the $\mathfrak{H}$-module generated by $R(\rho)^{\cdot} = R(\rho^{\cdot})$. Moreover, we can conclude from what we have seen above that, if σ is the representation of $H \cdot G$ in U, the isomorphism $U \rightarrow U^{\cdot}$ transports the representation $\sigma^{\cdot}$ of the Lie algebra $\mathfrak{H} + \mathfrak{G}$ of $H \cdot G$ to the representation of $\mathfrak{H} + \mathfrak{G}$ in $U^{\cdot}$ that we have used in the proof of Theorem 5.1. Thus *the representation of* $\mathfrak{H} + \mathfrak{G}$ *that is obtained in Theorem* 5.1 *may be identified with the differential of the representation of* $H \cdot G$ *that is obtained in Theorem* 3.1.

We can therefore apply Theorem 5.1 to conclude that, *if the representation of* H *in* $\mathfrak{G}$ *that is obtained from the adjoint representation of* $H \cdot G$ *is unipotent, then* H *is contained in the kernel of the representation* σ' *of Theorem* 3.1.

INSTITUTE FOR ADVANCED STUDY.

REFERENCES.

[0] C. Chevalley, *Theory of Lie groups*, Princeton, 1946.

[1] ———, *Théorie des groupes de Lie*, vol. III, Paris, 1955.

[2] M. Goto, "Faithful representations of Lie groups I," *Mathematicae Japonicae*, vol. 1 (1948), pp. 1-13.

[3] ———, "Faithful representations of Lie groups II," *Nagoya Mathematical Journal*, vol. 1 (1950), pp. 91-107.

[4] Harish-Chandra, "On the radical of a Lie algebra," *Proecedings of the American Mathematical Society*, vol. 1 (1950), pp. 14-17.

[5] G. Hochschild and G. D. Mostow, "Representations and representative functions of Lie groups," forthcoming in *Annals of Mathematics.*

[6] A. Malcev, "On linear groups," *Comptes rendus de l'Académie des Sciences de l'U.R.S.S.*, vol. 40 (1943), pp. 87-89.

[7] H. Zassenhaus, "Über die Darstellungen der Lie-Algebren bei Charakteristik 0," *Commentarii Mathematici Helvetici*, vol. 26 (1952), pp. 252-274.

NOTE ON CONVERGENCE OF THE PRODUCT OF BASIC SETS OF POLYNOMIALS.*

By M. NASSIF.

1. In his paper [1], W. F. Newns considered my note which appeared in this Journal some time ago [2]. Newns has shown that Theorem I of [2] is false and consequently, Theorem II, which depends for its proof on Theorem I, remains unproved. In the present note a modified version of the unproved Theorem II is established. For simplicity the notations used here, apart from those newly defined, are those of Newns paper to which the reader is referred.[1] Let $\{{}^*p_n(z)\}$ be the inverse of the W-basic set $\{p_n(z)\}$ [1; p. 455, l. 17] and let $M(r) = \lim\{M_n(r)\}^{1/n}$ as $n \rightarrow \infty$, if the limit exists. The result to be established is the following theorem.

THEOREM. *Let* $\{p_n^{(1)}(z)\}$ *be a* W*-basic set of polynomials and let* $\{p_n^{(2)}(z)\}$ *be another* W*-basic set for which*[2]

$$(1.1) \qquad d_n^{(2)} = O(n), \qquad {}^*d_n^{(2)} = O(n),$$

as n *tends to infinity. Suppose further that the set* $\{p_n^{(2)}(z)\}$ *is effective in* $|z| \leqq R$, *where*

$$(1.2) \qquad M^{(2)}(R) = aR, \qquad 0 < a < \infty\,; R > 0,$$

and that $\kappa^{(1)}(aR+)$ *is finite. Then the product set* $\{p_n(z)\}$ *of the two sets* $\{p_n^{(1)}(z)\}$ *and* $\{p_n^{(2)}(z)\}$, *in the given order, will be effective in* $|z| \leqq R$ *if, and only if, the set* $\{p_n^{(1)}(z)\}$ *is effective in* $|z| \leqq aR$.

In our notations, C denotes positive finite constants which are not generally of the same value at different occurrences, and ρ will be always written for aR. Now, for any set $\{p_n(z)\}$ satisfying (1.1), there exist finite numbers $\alpha > 1$, $\beta > 1$ such that

---

* Received March 5, 1956; revised January 20, 1957.

[1] Newns' notations used here are those defined in the following places of his paper: p. 445, l. 30; p. 446, ll. 8, 11, 23, 27-29; p. 447, l. 2; p. 455, l. 25; p. 458, ll. 7, 8 and finally p. 464, l. 16.

[2] Newns convention of notations [cf. 1; p. 456, l. 7] is adopted here also. Thus $d_n^{(2)}$ and ${}^*d_n^{(2)}$ are the degrees of the polynomials $p_n^{(2)}(z)$ and ${}^*p_n^{(2)}(z)$ respectively.

$$\text{(1.3a)} \quad d_n \leqq \alpha n, \qquad \text{(1.3b)} \quad {}^*d_n \leqq \beta n. \qquad (n \geqq 1)$$

The proof of the above theorem depends on two lemmas.

2. LEMMA 1. *Let* $\{p_n(z)\}$ *be a W-basic set which is effective in* $|z| \leqq R$, *where*

$$M(R) = \rho. \tag{2.1}$$

If ${}^*d_n = O(n)$, *then*

$${}^*M(\rho) = R. \tag{2.2}$$

If, moreover, $d_n = O(n)$ *then the inverse set* $\{{}^*p_n(z)\}$ *will be effective in* $|z| \leqq \rho$.

This lemma can be derived from Theorem 18.1 of Newns paper [cf. 1; pp. 459, 460]. For sake of completeness a direct proof is given here.

In fact, choosing a positive number $\rho_1 < \rho$ and finite numbers $\rho_2 > \rho$, $R_1 > R$ then it follows from (2.1) and the effectiveness of $\{p_n(z)\}$ in $|z| \leqq R$ that

$$\rho_1{}^n < CM_n(R) < C\rho_2{}^n \tag{2.3}$$

$$\omega_n(R) < CR_1{}^n. \qquad (n \geqq 0). \tag{2.4}$$

Hence, in view of (1.3b), (2.3) and (2.4) yield

$${}^*M_n(\rho) < \sum_k |\pi_{nk}| \rho^k < C(\rho/\rho_1)^{\beta n} R_1{}^n. \tag{2.5}$$

It readily follows, in view of (1.3a), that

$${}^*\omega_n(\rho) = \sum_k |p_{nk}| {}^*M_k(\rho) < C(\alpha n + 1)(\rho/\rho_1)^{\alpha\beta n} M_n(R_1). \tag{2.6}$$

Also, applying (1.3b) and (2.3) we obtain

$$R^n \leqq \omega_n(R) = \sum_k |\pi_{nk}| M_k(R) < C(\beta n + 1)\, {}^*M_n(\rho_2). \tag{2.7}$$

Now, from (1.3) and (2.1) it easily follows that

$$\mu(R_1)/R_1{}^\alpha \leqq \mu(R)/R^\alpha = \rho/R^\alpha; \quad {}^*\nu(\rho_2)/\rho_2{}^\beta \leqq {}^*\nu(\rho)/\rho^\beta. \tag{2.8}$$

Taking the n-th root and making n tend to infinity, (2.5), (2.7) and (2.6) respectively yield

$${}^*\mu(\rho) \leqq (\rho/\rho_1)^\beta R_1; \quad R \leqq {}^*\nu(\rho_2); \quad {}^*\lambda(\rho) \leqq (\rho/\rho_1)^{\alpha\beta} \mu(R_1).$$

Hence (2.8) gives

$$^*\mu(\rho) \leqq (\rho/\rho_1)^{\beta}R_1; \quad R \leqq (\rho_2/\rho)^{\beta}{}^*\nu(\rho); \quad {}^*\lambda(\rho) \leqq \rho(\rho/\rho_1)^{\alpha\beta}(R_1/R)^{\alpha}.$$

Finally, since R_1 can be taken as near to R as we please and ρ_1 and ρ_2 are taken arbitrarily near to ρ we conlclude that

$$^*\mu(\rho) \leqq R; \quad {}^*\nu(\rho) \geqq R; \quad {}^*\lambda(\rho) \leqq \rho.$$

The first two relations imply (2.2) and the third implies that the inverse set $\{^*p_n(z)\}$ is effective in $|z| \leqq \rho$; and the lemma is proved.

The following examples show that, in both assertions of the lemma the condition that $^*d_n = O(n)$ cannot be dropped, while if $^*d_n = O(n)$ and $\limsup_{n\to\infty} d_n/n = \infty$, (2.2) may hold although the inverse set may not be effective in $|z| \leqq \rho$.

Example 1. Let $m_k = 2^{2^k}$, where k is a positive integer or zero, and let c be a real number greater than 1. It is easily seen that, for the set $\{p_n(z)\}$, given by

$$p_{m_k}(z) = c^{-m_k^{\frac{1}{2}}}z^{m_k}; \quad p_n(z) = c^{-n^{\frac{1}{2}}}(z^n - z^{n+1}), \quad n \neq m_k; k \geqq 0,$$

$$M(r) = r; \quad r > 0, \quad d_n = O(n), \quad \limsup_{n\to\infty} {}^*d_n/n = \infty;$$

and that the set is effective in $|z| \leqq 1$. For the inverse set $\{^*p_n(z)\}$, it can be verified that $^*\mu(1) \geqq c > 1$, and that it is not effective in $|z| \leqq 1$.

Example 2. It is easily verified that the set $\{p_n(z)\}$, given by

$$p_{m_k}(z) = c^{-m_k^{\frac{1}{2}}}z^{m_k}; \quad p_n(z) = c^{-n^{\frac{1}{2}}}\sum_{j=n}^{m_{k+1}} z^j, m_k < n < m_{k+1}; \quad k \geqq 0,$$

where m_k and c are defined in Example 1, is effective in $|z| \leqq 1$ where $M(1) = 1$. It is also seen that $^*d_n = O(n)$, while $\limsup_{n\to\infty} d_n/n = \infty$. Now the inverse set $\{^*p_n(z)\}$ can be shown to be not effective in $|z| \leqq 1$ while $^*M(1) = 1$.

3. LEMMA 2. *Let* $\{p_n^{(1)}(z)\}$ *be any W-basic set of polynomials and let* $\{p_n^{(2)}(z)\}$ *be another W-basic set satisfying* (1.1) *and* (1.2). *Then, for the product set* $\{p_n(z)\}$, *we have*

$$\kappa(R+) \leqq \lambda^{(2)}(R)\{\kappa^{(1)}(\rho+)/\rho\}^{\beta}. \tag{3.1}$$

For let ρ' be any finite number greater than ρ and choose the numbers

ρ_1 and ρ_2 such that $0 < \rho_1 < \rho < \rho_2 < \rho' < \infty$. Then choosing the number $r > R$ such that $(r/R)^a < \rho_2/\rho$, it easily follows from (1.2), (1.3) and the properties of $\mu(r)$ that $\mu^{(2)}(r) < \rho_2$; so that

$$M_n^{(2)}(r) < C\rho_2^n \qquad (n \geqq 0). \tag{3.2}$$

Also, (1.2) implies that

$$\rho_1^n < CM_n^{(2)}(R) \qquad (n \geqq 0). \tag{3.3}$$

Now choose the integers s_n and t_n for the product set $\{p_n(z)\}$, so that

$$F_n(r) = \max_{|z|=r} \Big| \sum_{i=s_n}^{t_n} \pi_{ni} p_i(z) \Big| = \max_{|z|=r} \Big| \sum_k \pi_{nk}^{(2)} f_k(z) \Big|, \tag{3.4}$$

where $f_k(z) = \sum_{i=s_n}^{t_n} \pi_{ki}^{(1)} p_i(z)$. Write $g_k(z) = \sum_{i=s_n}^{t_n} \pi_{ki}^{(1)} p_i^{(1)}(z)$, then if $g_k(z) = \sum_j g_{kj} z^j$, it follows that

$$f_k(z) = \sum_j g_{kj} p_j^{(2)}(z). \tag{3.5}$$

Let $A_k(r) = \max_{|z|=r} |f_k(z)|$; applying Cauchy's inequality to $g_k(z)$ we easily obtain from (3.2) and (3.5),

$$A_k(r) < \sum_{j=0}^{\infty} M_j^{(2)}(r) F_k^{(1)}(\rho')/\rho'^j < CS(\rho_2, \rho') F_k^{(1)}(\rho'),$$

where $S(\rho_2, \rho')$ is bounded. Inserting this in (3.4) and applying (3.3) it follows that

$$\begin{aligned} F_n(r) &< \sum_k |\pi_{nk}^{(2)}| A_k(r) < CS(\rho_2, \rho') \sum_k |\pi_{nk}^{(2)}| M_k^{(2)}(R) F_k^{(1)}(\rho')/\rho_1^k \\ &< CS(\rho_2, \rho') \omega_n^{(2)}(R) F_{\sigma_n}^{(1)}(\rho')/\rho_1^{\sigma_n}, \end{aligned} \tag{3.6}$$

where $F_{\sigma_n}^{(1)}(\rho')/\rho_1^{\sigma_n} = \max_k F_k^{(1)}(\rho')/\rho_1^k > 1$. If σ_n remains finite as n tends to infinity, (3.6) yields

$$\kappa(r) \leqq \lambda^{(2)}(R). \tag{3.7}$$

If, on the other hand, $\limsup \sigma_n = \infty$, (3.6) gives, in view of (1.3),

$$\kappa(r) \leqq \lambda^{(2)}(R) \{\kappa^{(1)}(\rho')/\rho_1\}^{\beta}. \tag{3.8}$$

Finally, since ρ' and ρ_1 can be taken arbitrarily near to ρ, and since r tends to R as ρ' tends to ρ, the required relation (3.1) follows readily from (3.7) and (3.8).

4. *Proof of the Theorem.* Suppose that the set $\{p_n^{(2)}(z)\}$ satisfies the conditions of the theorem, and that $\kappa^{(1)}(\rho+)$ is finite. To prove the first part of the theorem suppose that the set $\{p_n^{(1)}(z)\}$ is effective in $|z| \leqq \rho$; then the known properties of $\kappa(r)$ [cf. 1; p. 449, Theorem 11.3] imply that $\kappa^{(1)}(\rho+) = \rho$ and (3.1) of Lemma 2 shows that $\kappa(R) = R$, so that the product set $\{p_n(z)\}$ is effective in $|z| \leqq R$.

To complete the proof of the theorem we first note that since $\kappa^{(1)}(\rho+)$ is finite and the set $\{p_n^{(2)}(z)\}$ is effective in $|z| \leqq R$, (3.1) implies that $\kappa(R+)$ is finite. Also Lemma 1 implies that the inverse set $\{{}^*p_n^{(2)}(z)\}$ is effective in $|z| \leqq \rho$, where ${}^*M^{(2)}(\rho)$ exists and is equal to R. Suppose now that the product set $\{p_n(z)\}$ is effective in $|z| \leqq R$. As we can put $\{p_n^{(1)}(z)\} = \{p_n(z)\}\{{}^*p_n^{(2)}(z)\}$, then the set $\{p_n(z)\}$, as an outer set, and $\{{}^*p_n^{(2)}(z)\}$, as an inner set, both satisfy the conditions of the "if"-statement of the theorem for $|z| = \rho$ and with $1/a$ for a. Consequently the product set $\{p_n^{(1)}(z)\}$ will be effective in $|z| \leqq \rho$ and the theorem is therefore established.

It should be observed that to prove the "if"-statement of the theorem the condition that $d_n^{(2)} = O(n)$ can be dispensed with. In fact, with the procedure of Lemma 2, the exclusion of the above condition leads to the "weaker" relation $\kappa(R) \leqq \lambda^{(2)}(R)\{\kappa^{(1)}(\rho+)/\rho\}^{\beta}$, from which the "if"-statment of the theorem can be deduced. This result has been given by Newns [cf. 1; p. 464, Theorem 22.1]. The fact that the other condition, ${}^*d_n^{(2)} = O(n)$, cannot be dropped is illustrated by the following example.

Example 3. Let m_k and c be defined as in Example 1, and consider the sets $\{p_n^{(1)}(z)\}$, $\{p_n^{(2)}(z)\}$ given by

$$p_n^{(1)}(z) = z^n, \quad (n \text{ even}); \quad p_n^{(1)}(z) = z^n - c^{(n+1)^{\frac{1}{2}}} z^{n+1}, \quad (n \text{ odd});$$

$$p_{m_k}^{(2)}(z) = z^{m_k}; \quad p_n^{(2)}(z) = z^n - z^{n+1}, \quad n \neq m_k; \quad k \geqq 0.$$

The set $\{p_n^{(1)}(z)\}$ is effective in $|z| \leqq r$ and $\kappa^{(1)}(r)$ is finite for $r > 0$. Also it is seen that the set $\{p_n^{(2)}(z)\}$ satisfies the conditions of the theorem for $0 < r \leqq 1$ and with $a = 1$, except that $\limsup_{n\to\infty} {}^*d_n^{(2)}/n = \infty$. The product set is easily seen to be not effective in $|z| \leqq 1$.

We finally append the following examples[3] to show that the theorem does not remain true if the condition $\kappa^{(1)}(aR+) < \infty$ is omitted or even weakened to $\kappa^{(1)}(aR+) = \kappa^{(1)}(aR-)$.

---

[3] These examples were suggested to me by the referee.

Example 4. Let $\{p_n(z)\}$ be the product of $\{p_n^{(1)}(z)\}$ and $\{p_n^{(2)}(z)\}$, where

$$p_n^{(1)}(z) = z^n \quad (n \text{ even}); \quad p_n^{(1)}(z) = z^n + z^{2n^2} \qquad (n \text{ odd});$$

$$p_0^{(2)}(z) = 1, \quad p_n^{(2)}(z) = n^{n\frac{1}{2}} + z^n \quad (n \text{ even} > 0); \quad p_n^{(2)}(z) = z^n \quad (n \text{ odd}).$$

The inner set is a simple set with leading coefficient unity, effective in $|z| \leqq r$ for all $r \geqq 1$. The outer set is effective in $|z| \leqq r$ for $r \leqq 1$, but $\kappa^{(1)}(1+) = \infty$. Now we find that

$$p_0(z) = 1, \; p_n(z) = n^{n\frac{1}{2}} + z^n \quad (n \text{ even} \geqq 0), \; p_n(z) = (2n^2)^{2\frac{1}{2}n} + z^n + z^{2n^2},$$

$(n$ odd), and that $\kappa(r) = \infty$ for all r.

Example 5. Consider now the product set $\{p_n^{(1)}(z)\} = \{p_n(z)\}\{{}^*p_n^{(2)}(z)\}$ where $\{p_n^{(1)}(z)\}$ and $\{p_n^{(2)}(z)\}$ are given in Example 4. The inner set satisfies the hypotheses of the theorem at $R = 1$ with $a = 1$. The outer set is no where effective, in fact $\kappa(1-) = \kappa(1+) = \infty$. However, the product set $\{p_n^{(1)}(z)\}$ is effective in $|z| \leqq 1$.

Finally, I should like to express my thanks to the referee of this note for the examples provided by him and for his other helpful and constructive suggestions.

Assiut University,
Assiut, Egypt.

REFERENCES.

[1] W. F. Newns, "On the representation of analytic functions by infinite series," *Philosophical Transactions of the Royal Society of London*, ser. A, vol. 245 (1953), pp. 429-468.

[2] M. N. Ghabbour, "On convergence of the product of basic sets of polynomials," *American Journal of Mathematics*, vol. 69 (1947), pp. 583-591.

A PROOF OF THE UNIQUENESS OF MINKOWSKI'S PROBLEM FOR CONVEX SURFACES.*

By SHIING-SHEN CHERN.

For C'' closed convex surfaces in ordinary Euclidean space E the uniqueness of Minkowski's problem says that the knowledge of the Gaussian curvature (supposed to be strictly positive) as a function of the unit normal vector determines the surface up to a translation. Let S_0 be the unit sphere about the origin 0 in E. Since the normal map onto S_0 of a convex surface M with Gaussian curvature $K > 0$ is one-one, M can be defined by a vector-valued function $x(\xi)$, $\xi \in S_0$.

Let T be the space of all right-handed rectangular frames $0e_1e_2e_3$ about 0. Then T is a circle bundle over S_0, the projection being defined by mapping the frame into the end-point of the last vector e_3. Let $\theta_{ij} = -\theta_{ji} = de_ie_j$. (Throughout this note small Latin indices run from 1 to 3 and small Greek indices from 1 to 2.) Then we have

$$d\theta_{ij} = \sum_k \theta_{ik} \wedge \theta_{kj}. \tag{1}$$

On the other hand, let F be the space of all right-handed rectangular frames $xf_1f_2f_3$ in E ($\dim F = 6$). If we put

$$\omega_i = dx \cdot f_i, \qquad \omega_{ij} = -\omega_{ji} = df_if_j, \tag{2}$$

or

$$dx = \sum_i \omega_i f_i, \qquad df_i = \sum_j \omega_{ij} f_j, \tag{3}$$

we have

$$d\omega_i = \sum_j \omega_j \wedge \omega_{ji}, \qquad d\omega_{ij} = \sum_k \omega_{ik} \wedge \omega_{kj}. \tag{4}$$

The mapping $x\colon S_0 \to M$ defined by sending $\xi \in S_0$ into the point $x(\xi) \in M$ at which the unit normal vector is ξ induces a mapping $\tilde{x}\colon T \to F$, which sends the frame $0e_1e_2e_3$ to $x(e_3)e_1e_2e_3$. Let $\tilde{\omega}_i = \tilde{x}^*\omega_i$, $\tilde{\omega}_{ij} = \tilde{x}^*\omega_{ij}$ be the differential forms in T induced by $\tilde{x}$. Then we have $\tilde{\omega}_{ik} = \theta_{ik}$, $\tilde{\omega}_3 = 0$ and we can put

$$\tilde{\omega}_\alpha = \sum_\beta \lambda_{\alpha\beta}\theta_{\beta 3}, \qquad \lambda_{\alpha\beta} = \lambda_{\beta\alpha}. \tag{5}$$

where $\lambda_{11}\lambda_{22} - \lambda_{12}\lambda_{21} = 1/K(\xi)$.

---

* Received February 5, 1957.

Suppose there be a second convex surface M' defined by the vector-valued function $x'(\xi)$, with the same Gaussian curvature $K(\xi)$. We denote by dashes notions pertaining to M'. Then we have $\tilde\omega'_3 = \tilde\omega_3 = 0$, $\tilde\omega'_{ij} = \tilde\omega_{ij}$, and

$$(6) \qquad \tilde\omega'_\alpha = \sum_\beta \lambda'_{\alpha\beta}\theta_{\beta 3}, \qquad \lambda'_{\alpha\beta} = \lambda'_{\beta\alpha}.$$

It suffices to prove that $\tilde\omega'_\alpha = \tilde\omega_\alpha$. For then $\tilde x'\tilde x^{-1}: \tilde x(T) \to \tilde x'(T)$ will be a one-one map under which $\omega'_i = (\tilde x'\tilde x^{-1})^*\omega_i, \omega'_{ij} = (\tilde x'\tilde x^{-1})^*\omega_{ij}$. By a well-known theorem on moving frames (E. Cartan, La théorie des groupes finis et continus . . . Paris, 1937), $\tilde x'\tilde x^{-1}$ is the identity, if it is the identity for one frame of $\tilde x(T)$. But this can be achieved by a translation.

To complete the proof we derive from (3), (5), (6) the formula

$$d(x, x', dx') = p'(\tilde\omega_2 \wedge \tilde\omega'_1 - \tilde\omega_1 \wedge \tilde\omega'_2) + 2p\tilde\omega'_1 \wedge \tilde\omega'_2$$
$$= \{p' \begin{vmatrix} \lambda'_{11} - \lambda_{11} & \lambda'_{12} - \lambda_{12} \\ \lambda'_{21} - \lambda_{21} & \lambda'_{22} - \lambda_{22} \end{vmatrix} + \frac{2}{K}(p - p')\}\theta_{13} \wedge \theta_{23}$$

where $p(\xi)$ is the distance from 0 to the tangent plane at $x(\xi)$. By Stokes Theorem we get

$$\int\int_{S_0} \{p' \begin{vmatrix} \lambda'_{11} - \lambda_{11} & \lambda'_{12} - \lambda_{12} \\ \lambda'_{21} - \lambda_{21} & \lambda'_{22} - \lambda_{22} \end{vmatrix} + \frac{2p}{K} - \frac{2p'}{K}\}\theta_{13} \wedge \theta_{23} = 0.$$

Since $(\lambda_{\alpha\beta})$ and $(\lambda'_{\alpha\beta})$ are positive definite symmetric matrices with the same determinant, it is well-known that

$$\begin{vmatrix} \lambda'_{11} - \lambda_{11} & \lambda'_{12} - \lambda_{12} \\ \lambda'_{21} - \lambda_{21} & \lambda'_{22} - \lambda_{22} \end{vmatrix} \leqq 0,$$

and that the equality sign holds only when $\lambda'_{\alpha\beta} = \lambda_{\alpha\beta}$. It follows that

$$\int\int_{S_0} \frac{1}{K}(p - p')\theta_{13} \wedge \theta_{23} \leqq 0$$

($p' < 0$, by choosing 0 to be in the interior of M'). But the relationship between M and M' is symmetrical, so that the relation still holds, when p and p' are interchanged. Hence the above integral is zero, and we have

$$\int\int_{S_0} p' \begin{vmatrix} \lambda'_{11} - \lambda_{11} & \lambda'_{12} - \lambda_{12} \\ \lambda'_{21} - \lambda_{21} & \lambda'_{22} - \lambda_{22} \end{vmatrix} \theta_{13} \wedge \theta_{23} = 0.$$

Here the integrand keeps a constant sign; the relation is possible, only when the integrand vanishes identically, which in turn implies $\lambda'_{\alpha\beta} = \lambda_{\alpha\beta}$. This completes our proof.

UNIVERSITY OF CHICAGO.

CORRESPONDENCE.*

A correspondent, who wishes to remain anonymous, writes as follows:

. . . . Una notissima congettura di F. Severi (*Rend. Pal.* 28 (1909), p. 45) asserisce che "*ogni varietà dotata di punti multipli si può considerare come limite di una senza singolarità, appartenente allo stesso spazio.*"

Secondo una notizia orora diffusa da Nancago dall'agenzia "United Press," l'ipotesi dell'illustre autore sarebbe stata confutata dall'egregio geometra francese Renato Thom, basandosi sull'esempio dei coni del 3° ordine nello spazio S_6 e mediante assai delicate considerazioni topologiche.

Forse non dispiacerà ai lettori del Suo pregiato periodico trovare qui una trattazione geometrica elementare dell'esempio di Thom. Di fatti, si determineranno tutte le varietà del 3° ordine in uno spazio S_n qualunque. Questo trarrà con sè, come conseguenza immediata, la falsità dell'ipotesi suddetta.

Sia V_r una varietà del 3° ordine nello spazio S_n, di dimensione $r < n-1$, non contenuta in un iperpiano. Sia C il cono, proiettante la V_r da un punto semplice qualunque M di V_r; sia M' un altro punto di V_r, semplice sul cono C. Il cono C è del secondo ordine; quindi la sua proiezione da M' è una varietà lineare di dimensione $r+1$, sicché la V_r è contenuta in una varietà lineare di dimensione $r+2$. È dunque $r=n-2$, e C hà la dimensione $n-1$. Lo stesso vale per il cono C', proiettante V_r da M'. I coni C, C' sono distinti, giacché M' è semplice sul cono C; la loro intersezione è dunque una varietà riducibile del 4° ordine, spezzata nella V_r e una varietà lineare. Siano $A=0$, $B=0$ le equazioni di quest'ultima. Allora si possono scrivere le equazioni dei coni C, C' nella forma:

$$AP=BQ, \qquad AP'=BQ', \tag{1}$$

denotando con P, Q, P', Q' quattro forme lineari nelle coordinate omogenee nello spazio. Sia s il numero di forme indipendenti fra le sei forme A, B, P, Q, P', Q'; questo è almeno 4, giacché, se fosse 2, i coni C, C' non sarebbero irriducibili, e, se fosse 3, la loro intersezione si spezzerebbe in quattro varietà lineari distinte o coincidenti. I valori possibili per s sono quindi 4, 5 e 6.

---

* Received June 3, 1957.

Sia L la varietà lineare, di dimensione $n-s$, definita dalle equazioni $A=B=0$, $P=Q=P'=Q'=0$. Ogni varietà lineare, proiettante da L un punto dell'intersezione di C e C', è contenuta in questa, come si vede subito sulle equazioni (1). Proiettando V_r da L, si ottiene quindi una varietà W del 3° ordine di dimensione $s-3$ in uno spazio S_{s-1}; e V_r non è altro che il cono proiettante W da L. Nello spazio S_{s-1}, si può prendere per coordinate omogenee s forme indipendenti fra le forme A, B, P, Q, P', Q'; allora le equazioni (1) vi definiscono una varietà del 4° ordine, spezzata nella W e una varietà lineare. Adesso distinguiamo tre casi:

(a) $s=6$: W è la varietà di Segre W_3 immersa in S_5, immagine birazionale senza eccezione del prodotto di un piano e una retta; come è noto, è priva di punti multipli.

(b) $s=5$: W è sezione iperpiana della sopradetta W_3. È facile vedere che tutte le sezioni iperpiane irriducibili della W_3 sono proiettivamente equivalenti fra di loro; denotando con W_2 una di esse, è anch'essa una varietà razionale senza punti multipli.

(c) $s=4$: W è la ben nota cubica razionale W_1 immersa in S_3.

Così è dimostrato che ogni varietà del 3° ordine appartiene a uno dei seguenti tipi:

1° le varietà di dimensione r, contenute in una varietà lineare di dimensione $r+1$;

2° le tre varietà razionali W_3, W_2, W_1 enumerate disopra;

3° i coni proiettanti una di queste tre da una varietà lineare di dimensione qualunque.

Evidentemente, una varietà del secondo o terzo tipo non può essere limite di una varietà del primo tipo, e perciò una varietà del terzo tipo, di dimensione maggiore di 3, non può essere limite di varietà prive di punti multipli.

X. X. X.